OfficeConnect®
ADSL Wireless 108Mbps 11g Firewall Router User Guide

Model WL-553
3CRWDR200A-75
3CRWDR200B-75

The Standard for Wireless Fidelity.

www.3Com.com
Part Number: 10015251 Rev. AA
Published June, 2006

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

Copyright © 2006, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, OfficeConnect and the 3Com logo are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

Wi-Fi and the Wi-Fi logo are registered trademarks of the WI-Fi Alliance.

IEEE and 802 are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

ABOUT THIS GUIDE

Naming Convention 7
Conventions 8
Feedback about this User Guide 9
Related Documentation 9

1 INTRODUCING THE ROUTER

OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router 11
Firewall Router Advantages 13
Package Contents 13
Minimum System and Component Requirements 15
Front Panel 15
Rear Panel 17

2 HARDWARE INSTALLATION

Introduction 19
Safety Information 19
Positioning the Router 19
Using the Rubber Feet 20
Stacking the Router 20
Wall Mounting 20
Before you Install your Router 21
Powering Up the Router 22
Connecting the Router 23

3 SETTING UP YOUR COMPUTERS

Obtaining an IP Address Automatically 25
Windows 2000 25
Windows XP 27

Windows 95/98/ME 27
Macintosh 27
Disabling PPPoE and PPTP Client Software 28
Disabling Web Proxy 28

4 RUNNING THE SETUP WIZARD

Accessing the Wizard 29
Password 32
Time Zone 33
ATM PVC Configuration 33
IGMP 34
Connection Mode 34
LAN Settings 39
Wireless Settings 41
Summary 42

5 ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages 45
Main Menu 45
Option Tabs 46
Welcome Screen 46
Notice Board 47
Password 47
Wizard 48
LAN Settings 49
Unit Configuration 49
DHCP Lease Table 50
Wireless Settings 50
Configuration 51
Encryption 53
Configuring WPA/WPA2 Encryption 54
Configuring WEP Encryption 56
WMM 58
Connection Control 59
Advanced Wireless Settings 60
Internet Settings 61
Firewall 62

Virtual Servers 62
Special Applications 63
Virtual DMZ 64
SPI 65
Internet Access Policy 67
Content Filter 69
System Tools 70
Restart 70
Time Zone 71
Configuration 72
Upgrade 73
Advanced 73
Routing 74
Static Route 74
RIP 75
DNS 77
DDNS 77
DSL 79
IPSec 79
Proxy ARP 80
ALG 81
Management 82
Syslog 82
SNMP 83
Trusted Station 84
Remote Management 84
Diagnostics 85
Device Info 86
Summary 86
WAN 86
Statistics 87
Route 87
ARP 88
Support/Feedback 88
Support 89
Feedback 89

6 TROUBLESHOOTING

Basic Connection Checks 91
Browsing to the Router Configuration 91
Connecting to the Internet 92
Forgotten Password and Reset to Factory Defaults 93
Wireless Networking 94
    Replacement Power Adapters 96
Alert LED 97
Recovering from Corrupted Software 97
Frequently Asked Questions 98

A USING THE 3COM DISCOVERY TOOL

Running the Discovery Application 101
    Windows Installation (95/98/2000/Me/NT) 101

B IP ADDRESSING

The Internet Protocol Suite 103
Managing the Router over the Network 103
    IP Addresses and Subnet Masks 103
How does a Device Obtain an IP Address and Subnet Mask? 105
    DHCP Addressing 105
    Static Addressing 105
    Auto-IP Addressing 106

C SAFETY INFORMATION

D END USER SOFTWARE LICENSE AGREEMENT

E ISP INFORMATION

GLOSSARY

REGULATORY NOTICES FOR THE ADSL WIRELESS 108MBPS 11G FIREWALL ROUTER

INDEX

About This Guide

This guide describes how to install and configure the OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router (3CRWDR200A-75 and 3CRWDR200B-75).

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Router systems.

If a release note is shipped with the OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router and contains information that differs from the information in this guide, follow the information in the release note.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

http://www.3com.com

Naming Convention

Throughout this guide, the OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router is referred to as the “Router”.

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 Text Conventions

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document product number (on the title page)
- Page number (if appropriate)

Example:

- OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router User Guide
- Product Number 3CRWDR200A-75
- Page 24

Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to the Support and Safety Information sheet.

Related Documentation

In addition to this guide, each Router document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Router.

1 INTRODUCING THE ROUTER

Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage. The OfficeConnect® product range from 3Com has changed all this, bringing networks to the small office.

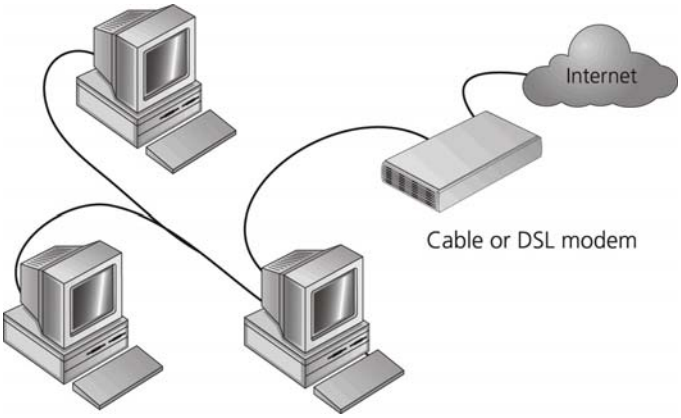
The products that compose the OfficeConnect range give you, the small office user, the same power, flexibility, and protection that has been available only to large corporations. Now, you can network the computers in your office, connect them all to a single Internet outlet, and harness the combined power of all of your computers.

OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router

The OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router is designed to provide a cost-effective means of sharing a single broadband Internet connection amongst several wired and wireless computers. The Router also provides internet services with standardized mechanism; namely, NAT and IPSec, etc. Thus, it further prevents anyone outside of your network from seeing your files or damaging your computers. The Router also gives you many administrative features such as scheduled internet access policies, web content filter, and intrusion detections.

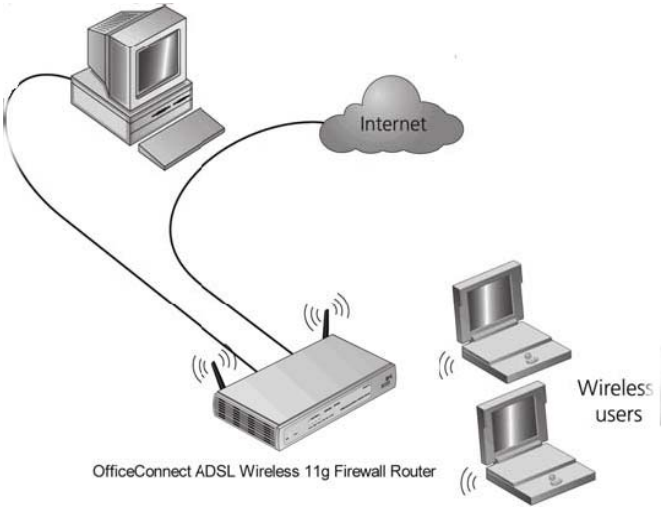
Figure 1 shows an example network without a Router. In this network, only one computer is connected to the Internet. This computer must always be powered on for the other computers on the network to access the Internet.

Figure 1 Example Network Without a Firewall Router



When you use the Firewall Router in your network (Figure 2), it becomes your connection to the Internet. Connections can be made directly to the Router, or to an OfficeConnect Switch or Hub, expanding the number of computers you can have in your network.

Figure 2 Example Network Using a ADSL Wireless 108Mbps 11g Firewall Router



Firewall Router Advantages

The advantages of the Firewall ADSL Wireless 108Mbps 11g Firewall Router include:

- Shared Internet connection for both wired and wireless computers
- High speed 802.11g wireless networking
- No need for a dedicated, “always on” computer serving as your Internet connection
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers
- Easy-to-use, Web-based setup and configuration
- Provides centralization of all network address settings (DHCP)
- Acts as a Virtual server to enable remote access to Web, FTP, and other services on your network
- Security — Firewall protection against Internet hacker attacks and encryption to protect wireless network traffic
- Filtered access of inappropriate Web sites using the built-in URL filter
- Internet Access Policy, to schedule your Internet Access rules with options in keywords and applications blocking
- Wireless Multimedia, to maximize the quality of your internet service with traffic prioritization

Package Contents

The Firewall Router kit includes the following items:

- One OfficeConnect ADSL Wireless 108Mbps 11g Firewall Router
- One power adapter for use with the Firewall Router
- Four rubber feet
- One RJ 11 cable (typically a telephone cable) if your model is 3CRWDR200A-75

- One RJ 45 cable (typically an Ethernet cable) if your model is 3CRWDR200B-75
- One Product Range Sheet
- One CD-ROM containing the Firewall Router Discovery program and this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer

If any of these items are missing or damaged, please contact your retailer.

Minimum System and Component Requirements

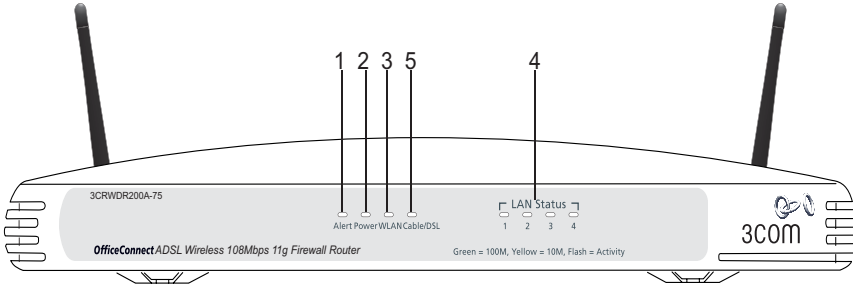
Your Router requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Router.
- An 802.11b or 802.11g wireless NIC.
- A cable modem or DSL modem with an Ethernet port (RJ-45 connector).
- An active Internet access account.
- A Web browser that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

Front Panel

The front panel of the Router contains a series of indicator lights (LEDs) that help describe the status of various networking and connection operations.

Figure 3 Router - Front Panel



1 Alert LED

Orange

Indicates a number of different conditions, as described below.

Off - The Router is operating normally.

Flashing quickly - Indicates one of the following conditions:

- The Router has just been started up and is running a self-test routine, or
- The administrator has invoked the *Reset to Factory Defaults* command, or
- The system software is in the process of being upgraded

In each of these cases, wait until the Router has completed the current operation and the alert LED is Off.

Flashing slowly - The Router has completed the *Reset to Factory Defaults* process, and is waiting for you to reset the unit. To do this, remove power, wait 10 seconds and then re-apply power. The Router will then enter the start-up sequence and resume normal operation.

If you have used a cable to reset the unit to Factory Defaults, See "Reset to Factory Default" on page 72.

On for 2 seconds, and then off - The Router has detected and prevented a hacker from attacking your network from the Internet.

Continuously on - A fault has been detected with your Router during the start-up process. Refer to Chapter 6 “Troubleshooting”.

2 Power LED

Green

Indicates that the Router is powered on.

3 Wireless LAN (WLAN) Status LED

Yellow

If the LED is on it indicates that wireless networking is enabled. If the LED is flashing, data is being transmitted or received. If the LED is off, the Wireless LAN has been disabled in the Router, or there is a problem. Refer to Chapter 6“Troubleshooting”.

4 Four LAN Status LEDs

Green (100 Mbps link) / yellow (10 Mbps link)

If the LED is on, the link between the port and the next piece of network equipment is OK. If the LED is flashing, the link is OK and data is being

transmitted or received. If the LED is off, nothing is connected, the connected device is switched off, or there is a problem with the connection (refer to Chapter 6 "Troubleshooting"). The port will automatically adjust to the correct speed and duplex.

5 Cable/DSL Status LED

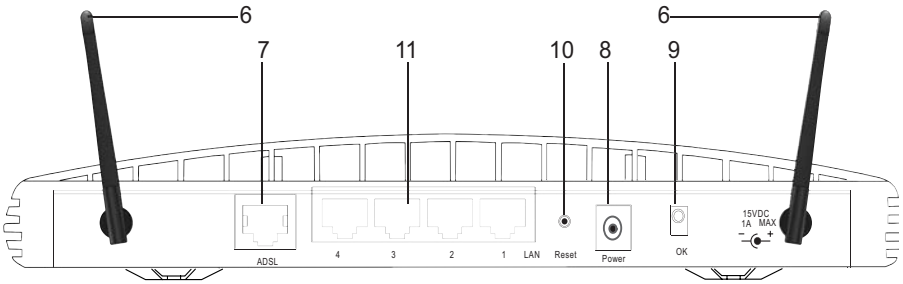
Green (100 Mbps link) / yellow (10 Mbps link)

If the LED is on, the link between the Router and the cable or DSL modem is OK. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, nothing is connected, the modem is switched off or there is a problem (refer to Chapter 6 "Troubleshooting").

Rear Panel

The rear panel (Figure 4) of the Router contains four LAN ports, one Ethernet Cable/DSL port, a power adapter OK LED, and a power adapter socket.

Figure 4 Router - Rear Panel



6 Wireless Antennae

The antennae on the product should be placed in a 'V' position when initially installed.

CAUTION: *Do not force the antennae beyond their mechanical stops. Rotating the antennae further may cause damage.*

7 ADSL port

Using the RJ11 cable provided, you should connect your Router to the telephone socket via a splitter.

8 Power Adapter Socket

Only use the power adapter supplied with this Router. Do not use any other adapter.

9 Power Adapter OK LED

Green

Indicates that the power adapter is supplying power to the Router. If the LED is off, there may be a problem with the power adapter or adapter cable.

10 Reset Button

Press this button for resetting your Router to factory default.

11 Four 10/100 LAN ports

Using suitable RJ-45 cable, you can connect your Router to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). The LAN ports will automatically set themselves to MDI or MDIX depending on the device to which they are connected and the type of cable used.

2 HARDWARE INSTALLATION

Introduction

This chapter will guide you through a basic installation of the Router, including:

- Connecting the Router to the Internet.
- Connecting the Router to your network.
- Setting up your computers for networking with the Router.

Safety Information

WARNING: *Please read the Router section in Appendix C before you start.*

VORSICHT: *Bitte lesen Sie den Abschnitt "Wichtige Sicherheitshinweise" sorgfältig durch, bevor Sie das Gerät einschalten.*

AVERTISSEMENT: *Veuillez lire attentivement la section "Consignes importantes de sécurité" avant de mettre en route.*

Positioning the Router

You should place the Router in a location that:

- is conveniently located for connection to the cable or DSL modem that will be used to connect to the Internet.
- is centrally located to the wireless computers that will connect to the Router. A suitable location might be on top of a high shelf or similar furniture to optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.
- allows convenient connection to the computers that will be connected to the four LAN ports on the rear panel, if desired.

- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.

When positioning your Router, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. 3Com recommends you provide a minimum of 25 mm (1 in.) clearance.

Using the Rubber Feet

Use the four self-adhesive rubber feet to prevent your Router from moving around on your desk or when stacking with other flat top OfficeConnect units. Only stick the feet to the marked areas at each corner of the underside of your Router.

Stacking the Router

If you are stacking your Router with other OfficeConnect units, install the Router at the top of the stack. Refer to the documentation supplied with your other OfficeConnect unit for details on using the stacking clip.

A stacking clip is not supplied with the Router. Use the stacking clip supplied with another stackable OfficeConnect unit.

Wall Mounting

There are two slots on the underside of the Router that can be used for wall mounting.

When wall mounting the unit, ensure that it is within reach of the power outlet. Don't install the Router more than 200 centimeter above the ground.

You will need two suitable screws to wall mount the unit. To do this:

1. Ensure that the wall you use is smooth, flat, dry and sturdy and make two screw holes which are 150 mm (5.9 in.) apart.
2. Fix the screws into the wall, leaving their heads 3 mm (0.12 in.) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.

When making connections, be careful not to push the unit up and off the wall.Router

CAUTION: *Only wall mount single units, do not wall mount stacked units.*

Before you Install your Router

Before you install and configure your Router, you need the following additional information. If you do not have this information, contact your Internet Service Provider (ISP). Space is provided below for you to record this information.

If you have a DSL connection and your ISP allocates IP information dynamically, you need a User Name and Password:

User Name	: _____
Password	: _____
Service Name	: _____
Authentication Method	: _____

You only need a PPPoE Service Name if your ISP requires one. Do not enter anything if your ISP does not require this information.

You should leave the Authentication Method as its default: Auto if your ISP doesn't specify this parameter.

If your ISP allocates fixed or static IP information, you need the following information:

IP Address : ____.____.____.____

Subnet Mask : ____.____.____.____

Default Router address : ____.____.____.____

DNS address : ____.____.____.____

If your ISP allocates IP information dynamically over a protocol other than PPPoE, you do not need any further information. This configuration is typical of cable connections.

Powering Up the Router

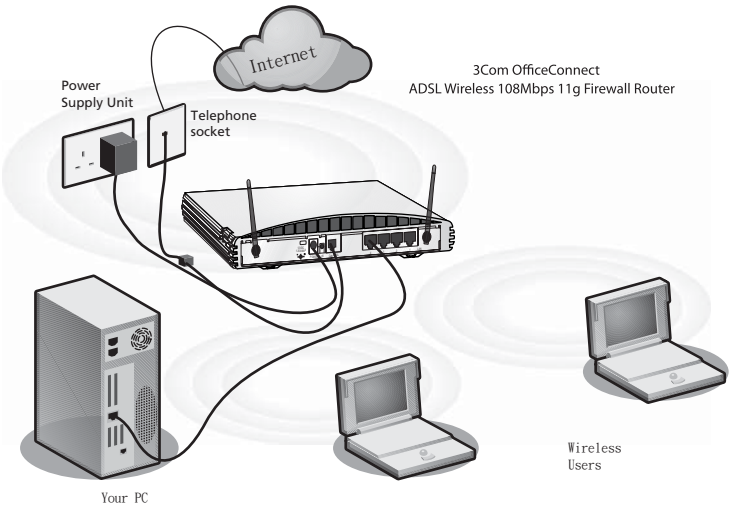
To power up the Router:

1. Plug the power adapter into the power adapter socket located on the back panel of the Router.
2. Plug the power adapter into a standard electrical wall socket.

Connecting the Router

The first step for installing your Router is to physically connect it to a RJ11 cable with the splitter and then connect the Router to a computer in order to be able to access the Internet. See Figure 5:

Figure 5 Connecting the Router



To use your Router to connect to the Internet through an DSL connection:

1 Insert one end of the supplied telephone (RJ-11) cable into the Cable/DSL port on the rear panel of the Router. Check that the DSL Sync status LED lights on the Router.

2 Connect your computer to one of the four LAN ports on the Router using a Category 5 twisted pair cable. Check that the corresponding LAN status LED on the Router lights.

You have now completed the hardware installation of your Router. Next you need to set up your computers so that they can make use of the Router to communicate with the Internet.

3Com recommends that you perform the initial Router configuration from a computer that is directly connected to one of the LAN ports.

If you configure the Router from a wireless computer, note that you may lose contact with the Router if you change the wireless configuration.

To communicate wirelessly with your Router, your wireless NIC should be set as follows:

- Encryption — none
- Service Area Name/SSID — 3Com
- Channel — 11

4 Running the Setup Wizard

Accessing the Wizard

The Firewall Router setup program is Web-based, which means that it is accessed through your Web browser (Netscape Navigator 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher).

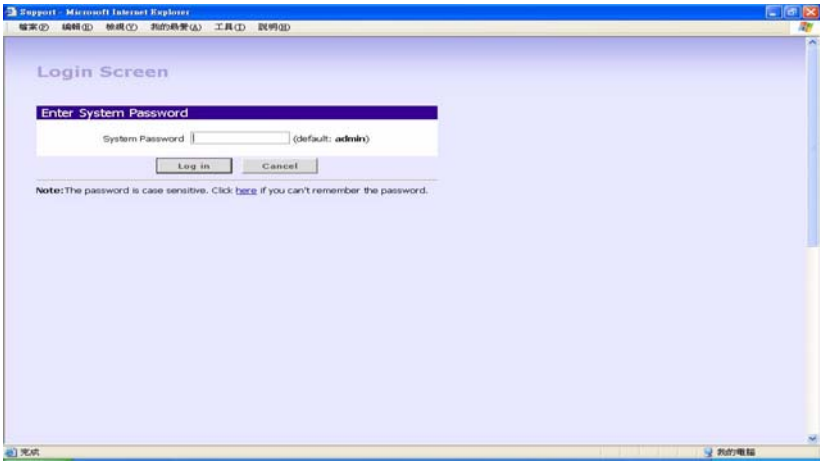
To use the Setup Wizard:

1. Ensure that you have at least one computer connected to the Firewall Router. Refer to Chapter 2 for details on how to do this.
2. Launch your Web browser on the computer.
3. Enter the following URL in the location or address field of your browser: **`http://192.168.1.1`** (Figure 9). The Login screen displays.

Figure 9 Web Browser Location Field (Factory Default)

4. To log in as an administrator, enter the password (the default setting is **admin**) in the *System Password* field and click *Log in* (Figure 10).

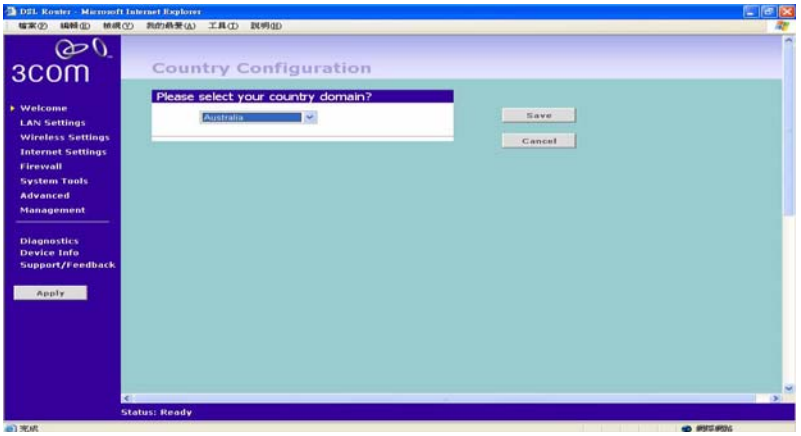
Figure 10 Firewall Router Login Screen



5 If the password is correct, the *Country Selection* screen will appear. Select the country you wish to configure the Firewall Router for, then click *Apply*. (Figure 11)

If your purchased your Firewall Router in the United States, you do not see this screen, as it is automatically set.

Figure 11 Country Selection Screen



6 When you have selected a country either:

■ The *Welcome* screen will appear (Figure 12). Select the *Wizard* tab and click *Wizard.*

or

■ If your Router has not been configured before, the Wizard will launch automatically (refer to Figure 13).

7 Click *Next*.

8 You will be guided step by step through a basic setup procedure.

Figure 12 Welcome Screen

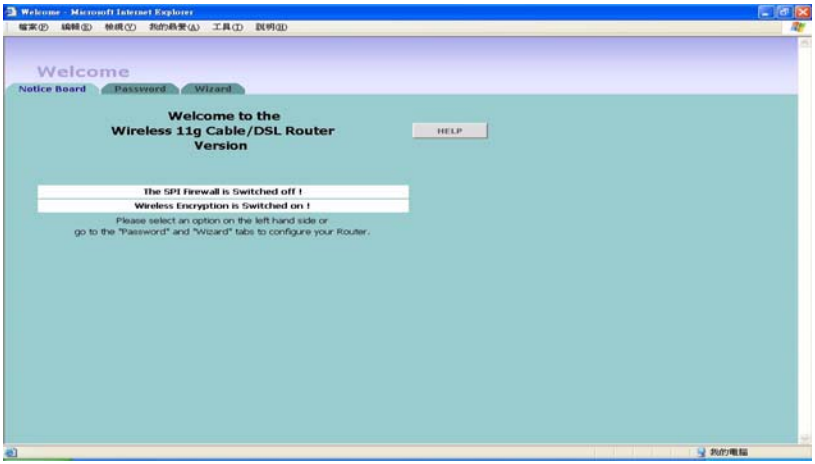
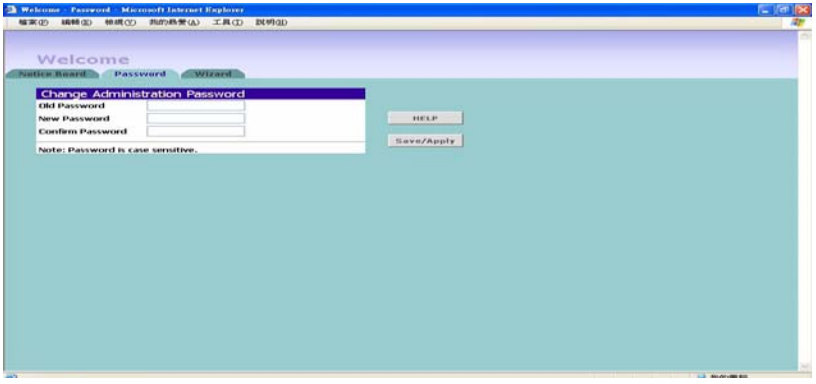

Welcome - Microsoft Internet Explorer
Welcome
Notice Board
Password
Wizard
Welcome to the
Wireless 11g Cable/DSL Router
Version
HELP
The SPI Firewall is Switched off !
Wireless Encryption is Switched on !
Please select an option on the left hand side or
go to the "Password" and "Wizard" tabs to configure your Router.

Figure 13 Wizard Screen

Password

Figure 14 Change Administration Password Screen



When the *Change Administration Password* screen (Figure 14) appears, type the *Old Password*, then a new password in both the *New Password* and *Confirm Password* boxes.

3Com recommends entering a new password when setting up the Firewall Router for the first time. The Firewall Router is shipped from the factory with a default password, **admin***.*

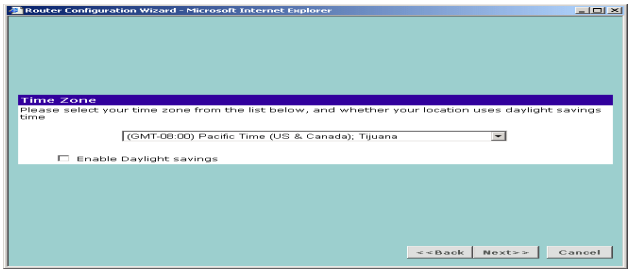
1. Password is case sensitive.

2. Write the new password down and keep it in a safe place, so that you can change your settings in the future.

Click *Next* to display the *Time Zone* setup screen (Figure 15).

Time Zone

Figure 15 Time Zone Screen


Router Configuration Wizard - Microsoft Internet Explorer
Time Zone
Please select your time zone from the list below, and whether your location uses daylight savings time
(GMT-08:00) Pacific Time (US & Canada); Tijuana
Enable Daylight savings
<<Back
Next>>
Cancel

Select your time zone from the pull-down menu, check the daylight savings option if required, and then click *Next*.

The Daylight Savings option advances the system clock by one hour. It does not cause the system clock to be updated for daylight savings time automatically.

ATM PVC Configuration

VPI stands for Virtual Path Identifier - contained in the ATM cell header to designate the virtual path on the physical ATM link.

VCI stands for Virtual Channel Identifier - 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination.

You may select on DSL Auto-connect or enter the values for VPI and VCI.

Quality of Service

Select the type of QoS from the drop-down list:

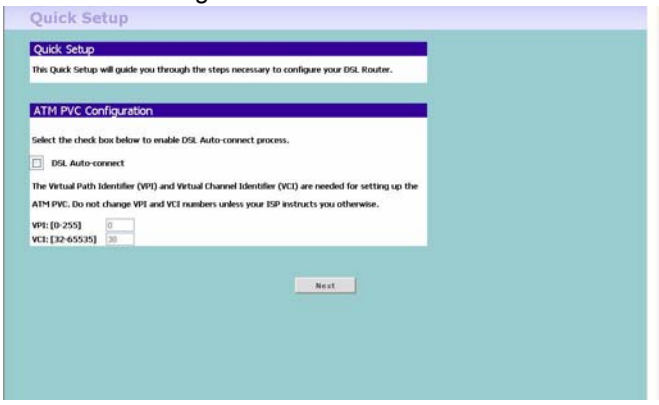
■ UBR (Unspecified Bit Rate) with/without PCR (Peak Cell Rate): the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer

communications applications. The UBR service may be considered as "best effort service". Peak cell rate specifies the maximum cell rate at which the user will transmit.

- CBR (constant bit rate): the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.

- VBR (Variable Bit Rate) is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Typical VBR sources are compressed voice and video. These applications require small delay variations.

Figure 16 The ATM Configuration screen


Quick Setup
Quick Setup
This Quick Setup will guide you through the steps necessary to configure your DSL Router.
ATM PVC Configuration
Select the check box below to enable DSL Auto-connect process.
DSL Auto-connect
The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 0
VCI: [32-65535] 35
Next

IGMP IGMP stands for Internet Group Management Protocol which is defined in RFC 1112 as the standard for IP Multicast.

Select to enable IGMP multicast.

Select to enable WAN service and enter the service name to identify your internet service.

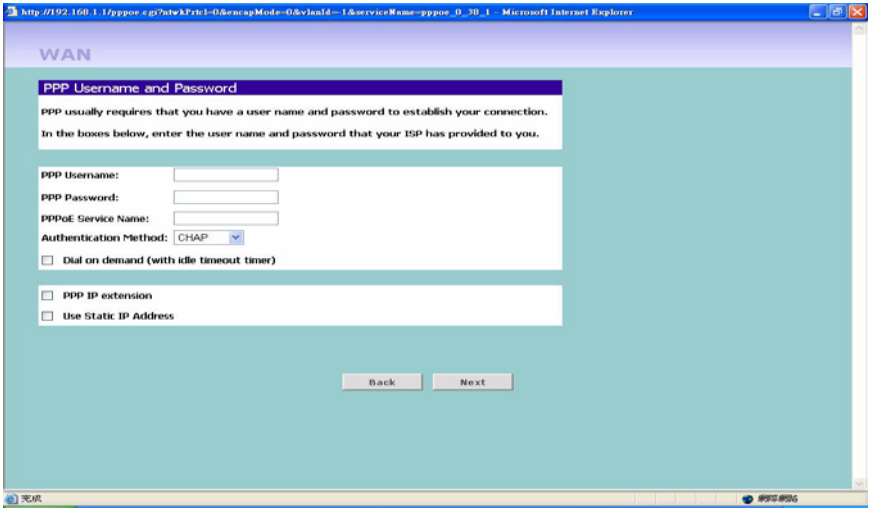
Connection Mode Select an Internet Addressing mode from the following:

- PPPoE/PPPoA is required (typically DSL users only) see page 35
- IP over ATM (IPoA, using ATM networks as the underlying data link for IP networks, defined by IETF RFC 1577) see page 38
- MAC Encapsulation Routing (MER) see page 37
- Bridging, see page 39

and click *Next*.

PPPoE/PPPoA Mode

Figure 17 PPPoE Screen


WAN
PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection.
In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
CHAP
Dial on demand (with idle timeout timer)
PPP IP extension
Use Static IP Address
Back
Next

To setup the Firewall Router for use with a PPP over Ethernet (PPPoE) or PPP over ATM (used mainly in UK) connection, use the following procedure:

1. Enter your PPP over Ethernet/ATM user name in the *PPPoE/PPPoA User Name* text box.
2. Enter your PPP over Ethernet/ATM password in the *PPPoE/PPPoA Password* text box.
3. Enter your PPP over Ethernet/ATM service name in the *PPPoE/PPPoA Service Name* text box.

Do not enter anything in this box if your ISP does not require a service name.

4 Select PPP Authentication Method from the drop-down menu.

5 Dial on Demand: Check the box to make a connection while in demand. Enter the *Inactivity Timeout* to cut off the network connection if there is no activity for this router.

6 PPP IP extension: Check this box to invoke the PPP IP extension. Only one user is allowed to access the web configurator at one time when this is checked.

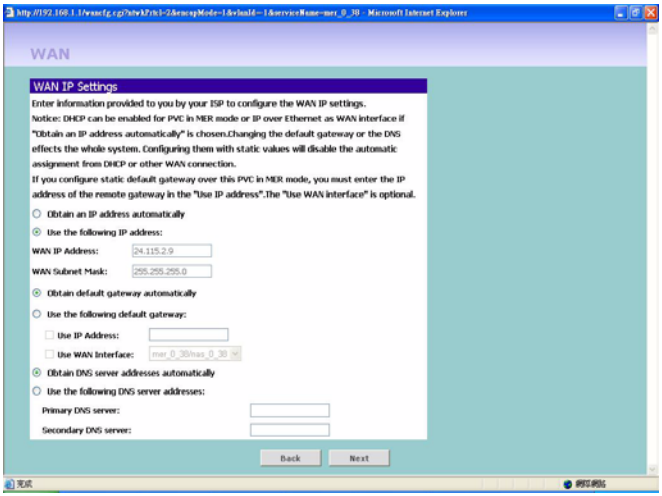
7 Use Static IP Address: Check this box to enter the IP Address manually. Check all of your settings, and then click *Next*.

Enable 802.1q

Check on this to enable this function. The 802.1q standard defines the *VLAN* protocol which allows insertion of a 4-byte identifier into the ethernet frame format to identify the VLAN to which the frame belongs. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local.You can configure the router to route traffic to the appropriate destination VLAN. To specify a VLAN interface, enter the *Vlan-id* in the field.

MER Mode

Figure 18 MER screen


WAN
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address".The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

MER mode is used in business environment where static IP address and subnet are assigned by your ISP. Choose MER and click Next.

To setup the Firewall Router for use with a MER connection, use the following procedure:

Obtain an IP address automatically: Click this button to make the system get an IP address automatically.

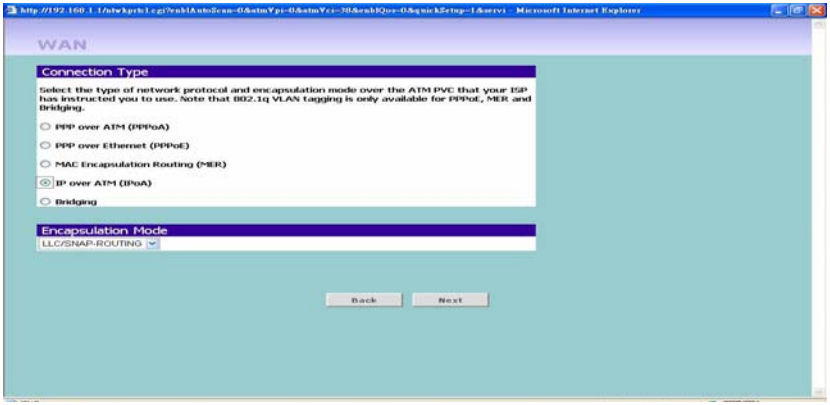
Manually entering an IP address: To set WAN IP address by yourself.

1. WAN IP Address: Enter the IP address for using in the WAN from your ISP.
2. WAN Subnet Mask: Enter the WAN subnet mask.
3. Default Gateway: Enter the default gateway for using in the WAN from your ISP.
4. Enter your primary DNS address in the *Primary DNS Address* text box.
5. Enter your secondary DNS address in the *Secondary DNS Address* text box.
6. Check all of your settings, and then click *Next or back* to go back to the pervious screen.

7 Configuring LAN setting: See "LAN Settings" in this section for more information.

IPoA Mode

Figure 19 IPoA Mode Screen


WAN
Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-ROUTING
Back
Next

To setup the Firewall Router for use with a IPoA connection, use the following procedure:

1 Enter the IP Address for WAN interface.

2 Enter the Subnet Mask for WAN interface.

3 Enter your *Primary DNS Address* and *Secondary DNS address*.

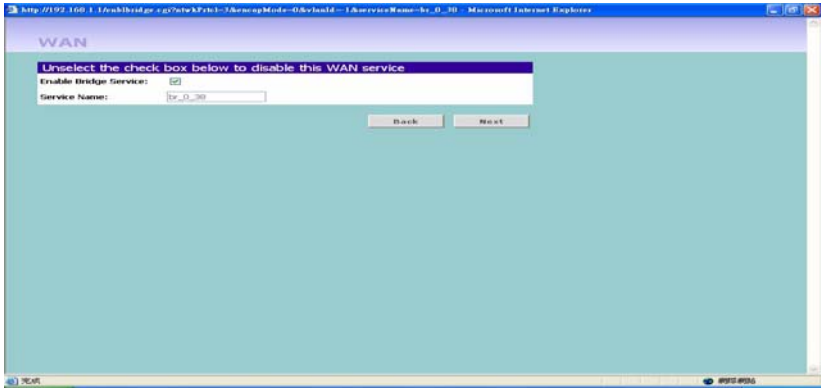
Your ISP may provide you with primary and secondary DNS addresses. If they have been provided, enter the addresses in the appropriate text boxes. If not, leave *0.0.0.0* in the boxes.

4 Enable NAT: Check the Enable NAT to enable this function which will allow more than one PC in the LAN to connect the internet.

5 Click on *Next* to configure your LAN settings. See "LAN Settings" in this section for more information.

Bridging Mode

Figure 20 Bridging Mode Screen

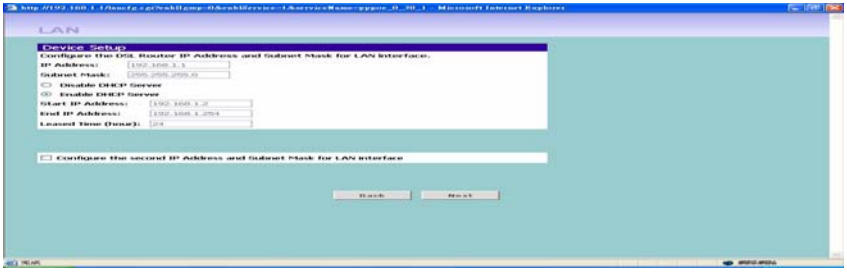


To set up the Firewall Router for use as a bridge in which the router is the bridge between WAN and LAN, use the following procedure:

1. Enter the name for the bridging service.
2. Enter the IP Address and Subnet Mask for the LAN. See "LAN Settings"

LAN Settings

Figure 21 LAN IP Address Screen



This screen displays a suggested LAN IP address and subnet mask of the Firewall Router. It also allows you to change the IP address and subnet mask.

1. Primary IP Address: Enter the first IP Address for your LAN interface.
2. Subnet Mask: Enter the Subnet Mask for your LAN interface.
3. Enable DHCP server on the LAN: Check this box to enable the DHCP service on the router. See "DHCP" in this section.

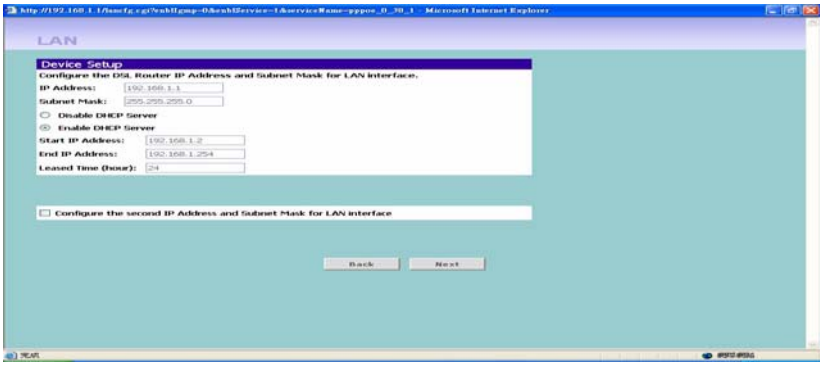
4 Configure the second IP Address and Subnet Mask for the LAN interface: Check this box to make another set of IP Address and Subnet Mask to connect to your router if they are not included in the range of DHCP server.

5 Enter the Secondary IP Address and Subnet Mask.

DHCP

The Firewall Router contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network.

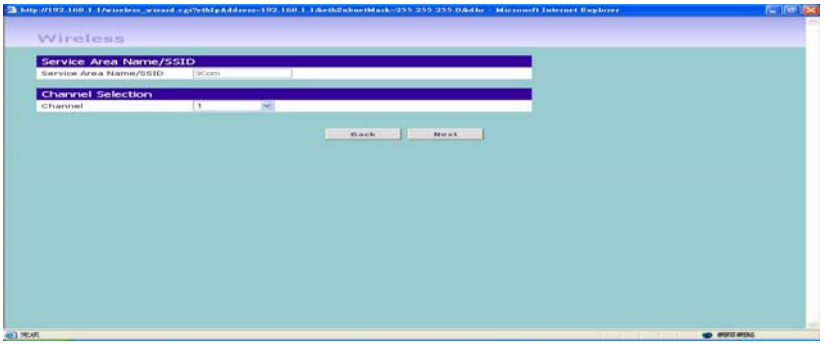
Figure 22 DHCP Server Setup Screen



To activate the DHCP Server option, select *Enable the DHCP server with the following settings:* Enter the *start and end IP Address* of your DHCP range. Enter the leased time in hour to specify the frequency for DHCP assignment.Check the *Enable DHCP Server Relay* to forward the DHCP request to another server. Enter the IP Address of the designated server.

Wireless Settings

Figure 23 Wireless Configuration Screen



This screen displays the Channel and Service Area Name. It also allows you to change these settings. There are a maximum of 14 channels, the number available to you is dependent on the country you reside in. Selecting *Clear Channel Select* from the *Channel* drop-down list allows the Firewall Router to automatically select an available channel when first powered on.

The Service Area Name default for 3Com products is “3Com”. Up to 32 (case sensitive) characters can be entered for the Service Area Name.

3Com strongly recommends that you change the SSID to something other than the default.

Click *Next* when you have finished.

If you are configuring the Firewall Router from a wireless computer any changes you make to the wireless configuration will result in communication between the Firewall Router and your computer being lost. This is why 3Com strongly recommends that you configure the Firewall Router from a wired computer.

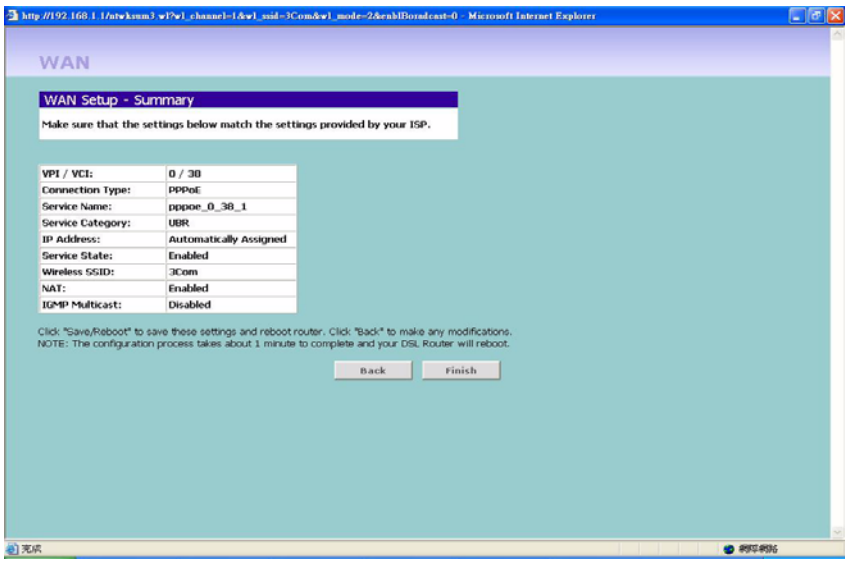
It is very important that you set up your wireless clients to use the same Service Area Name or SSID as the one you use on this screen. If your clients use a different Service Area Name then they will not be able to communicate with the Firewall Router.

The choice of channel is less important as Clients will generally search all of the available channels. You should however make a note of the

channel you select as this may be useful if you experience problems with your clients.

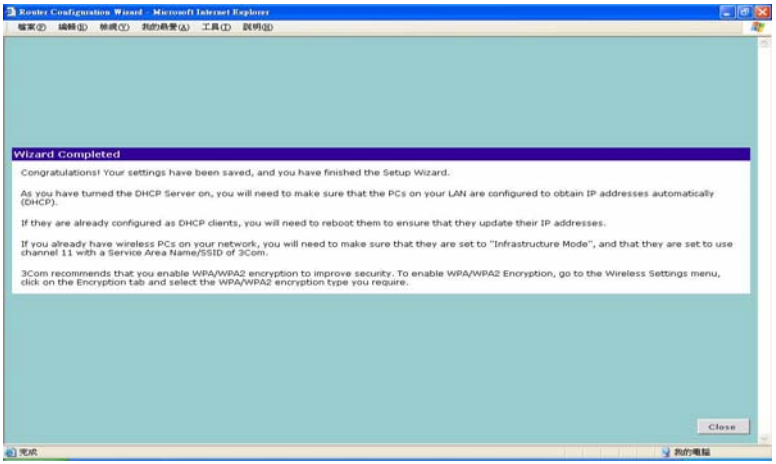
Summary

Figure 24 Configuration Summary Screen


WAN
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
VPI / VCI: 0 / 38
Connection Type: PPPoE
Service Name: pppoe_0_38_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
Wireless SSID: 3Com
NAT: Enabled
IGMP Multicast: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Finish

When you complete the Setup Wizard, a configuration summary will display. 3Com recommends that you verify the configuration information of the Firewall Router and then print this page for your records. Click *Finish* to display the Wizard completed screen, shown in Figure 25

Figure 25 Wizard Completed Screen


Router Configuration Wizard - Microsoft Internet Explorer
Wizard Completed
Congratulations! Your settings have been saved, and you have finished the Setup Wizard.
As you have turned the DHCP Server on, you will need to make sure that the PCs on your LAN are configured to obtain IP addresses automatically (DHCP).
If they are already configured as DHCP clients, you will need to reboot them to ensure that they update their IP addresses.
If you already have wireless PCs on your network, you will need to make sure that they are set to "Infrastructure Mode", and that they are set to use channel 11 with a Service Area Name/SSID of 3Com.
3Com recommends that you enable WPA/WPA2 encryption to improve security. To enable WPA/WPA2 Encryption, go to the Wireless Settings menu, click on the Encryption tab and select the WPA/WPA2 encryption type you require.
Close

If you have made changes to the LAN Settings or wireless configuration options, you may need to reconfigure the computer you are using in order to make contact with the Firewall Router again.

Your Firewall Router is now configured and ready for use.

For information on improving your Wireless network security see "Wireless Settings" on page 50.

See Chapter 5 for a detailed description of the Router configuration screens.

3 SETTING UP YOUR COMPUTERS

The Router has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter. If your computers are configured with fixed or static addresses and you do not wish to change this, then you should use the Discovery program on the Router CD-ROM to detect and configure your Router. Refer to Appendix A for information on using the Discovery program.

Obtaining an IP Address Automatically

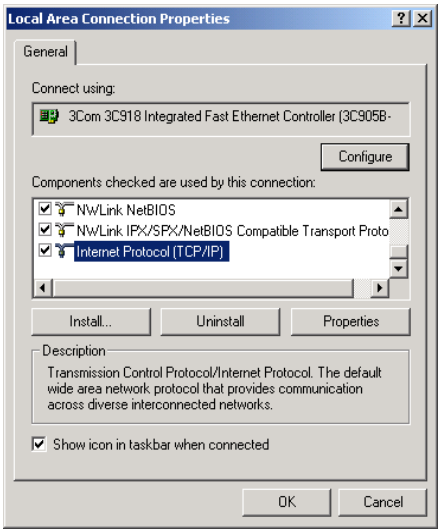
Refer to the section below which relates to your operating system for details on how to obtain an IP address automatically.

Windows 2000

If you are using a Windows 2000-based computer, use the following procedure to change your TCP/IP settings:

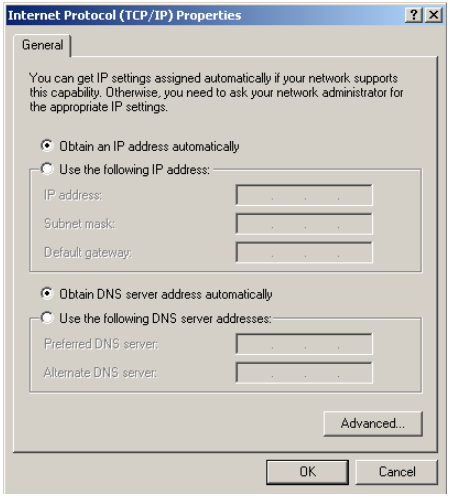
1. From the Windows *Start* Menu, select *Settings* > *Control Panel*.
2. Double click on *Network and Dial-Up Connections*.
3. Double click on *Local Area Connection*.
4. Click on *Properties*.
5. A screen similar to Figure 6 should be displayed. Select *Internet Protocol TCP/IP* and click on *Properties*.

Figure 6 Local Area Properties Screen



6 Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS server address automatically* are both selected as shown in Figure 7. Click *OK*.

Figure 7 Internet Protocol (TCP/IP) Properties Screen


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

7 Restart your computer.

Windows XP If you are using a Windows XP computer, use the following procedure to change your TCP/IP settings:

1. From the Windows *Start* menu, select *Control Panel*.
2. Click on *Network and Internet Connections*.
3. Click on the *Network Connections* icon.
4. Double click on *LAN* or *High Speed Connection* icon. A screen titled *Local Area Connection Status* will appear.
5. Select *Internet Protocol TCP/IP* and click on *Properties*.
6. Ensure that the options *Obtain an IP Address automatically*, and *Obtain DNS servers automatically* are both selected. Click *OK*.
7. Restart your computer.

Windows 95/98/ME If you are using a Windows 95/98/ME computer, use the following procedure to change your TCP/IP settings:

1. From the Windows *Start* Menu, select *Settings* > *Control Panel*.
2. Double click on *Network*. Select the *TCP/IP* item for your network card and click on *Properties*.
3. In the TCP/IP dialog, select the *IP Address* tab, and ensure that *Obtain IP address automatically* is selected. Click *OK*.

Macintosh If you are using a Macintosh computer, use the following procedure to change your TCP/IP settings:

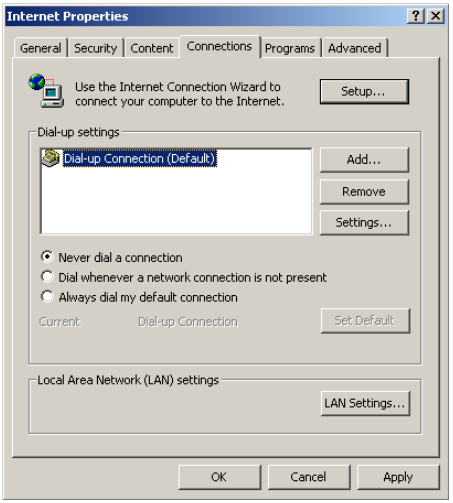
1. From the desktop, select *Apple Menu*, *Control Panels*, and *TCP/IP*.
2. In the *TCP/IP* control panel, set *Connect Via:* to “Ethernet”.
3. In the TCP/IP control panel, set *Configure:* to “Using DHCP Server.”
4. Close the *TCP/IP* dialog box, and save your changes.
5. Restart your computer.

Disabling PPPoE and PPTP Client Software

If you have PPPoE or PPTP client software installed on your computer, you will need to disable it. To do this:

1. From the Windows *Start* menu, select *Settings* > *Control Panel*.
2. Double click on *Internet* Options.
3. Select the *Connections* Tab. A screen similar to Figure 8 should be displayed.
4. Select the *Never Dial a Connection* option.

Figure 8 Internet Properties Screen



You may wish to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Router.

Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click *LAN Settings* at the bottom. Make sure that the *Use Proxy Server* option is unchecked.

5 ROUTER CONFIGURATION

Navigating Through the Router Configuration Pages

This chapter describes all the screens available through the Router configuration pages, and is provided as a reference. To get to the configuration pages, browse to the Router by entering the URL in the location bar of your browser. The default URL is `http://192.168.1.1` but if you changed the Router LAN IP address during initial configuration, use the new IP address instead. When you have browsed to the Router, log in using your system password (default *admin*).

Main Menu

At the left side of all screens is a main menu, as shown in Figure 26 on page 47. When you click on a topic from the main menu, that page will appear in the main part of the screen.

- Welcome — displays the firmware version of the Router, allows you to change your password, and launch the Wizard

- LAN Settings — allows you to configure the LAN interface and view the leased DHCP client list.

- Wireless Settings — enables /disables access from wireless computers, configures WPA or WEP encryption, provides facilities for improving the security of the wireless network, setup WMM parameters, Wireless mode selection, Mac Access Control and Advanced Wireless Settings.

- Internet Settings — let you set up the WAN (Wide Area Network) ie. DSL Moden connection.

- Firewall — allows configuration of the Router's firewall features: Virtual Servers, Special Applications, DMZ Hosts, SPI options, Internet Access Policy, and Content Filtering.

- System Tools — allows the administrator to perform maintenance activities on the Router.

- Advanced — allows the administrator to monitor and configure the Router's advanced features, including Static Routing, DSL, RIP, DDNS, IPSec, Proxy ARP, and ALG.

- Management — displays the current status and activity logs of the Router, SNMP enable/disable, Internet service enable/disable, and remote management control.

- Diagnostics — Testing the connection between your wired and wireless device to your Router.

- Device Info — Providing the configuration summary and statistics on your LAN/WAN/ATM/ADSL connection.

- Support/Feedback — contains a comprehensive online help system and allows you to provide 3Com with feedback on your Router.

Option Tabs

Each corresponding menu page may also provide sub-sections which are accessed through the use of tabs (see Figure 26 for example). To access a sub-section, simply click on the required tab.

Getting Help

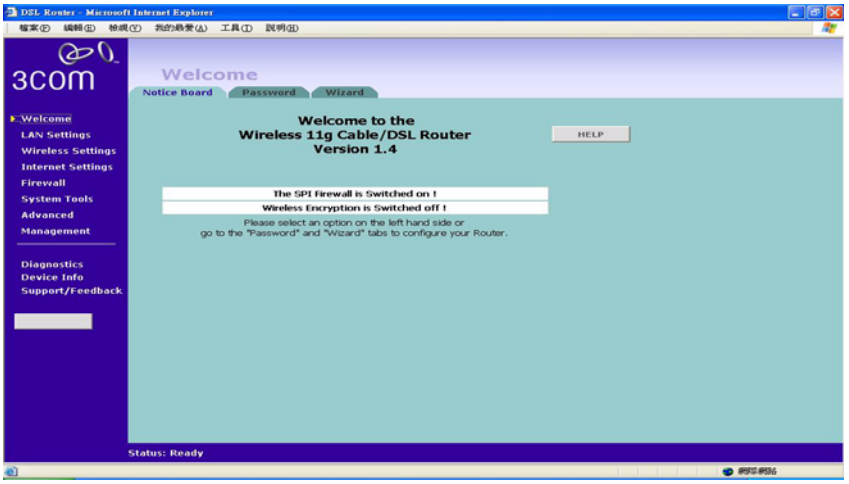
On every screen, a Help button is available which provides access to the context-sensitive online help system. Click *Help* for further assistance and guidance relating to the current screen.

Welcome Screen

The *Welcome* section allows you to view the Notice board and to change your Password. You can also gain access to the Configuration Wizard. (See "Accessing the Wizard" on page 29 for details).

Notice Board

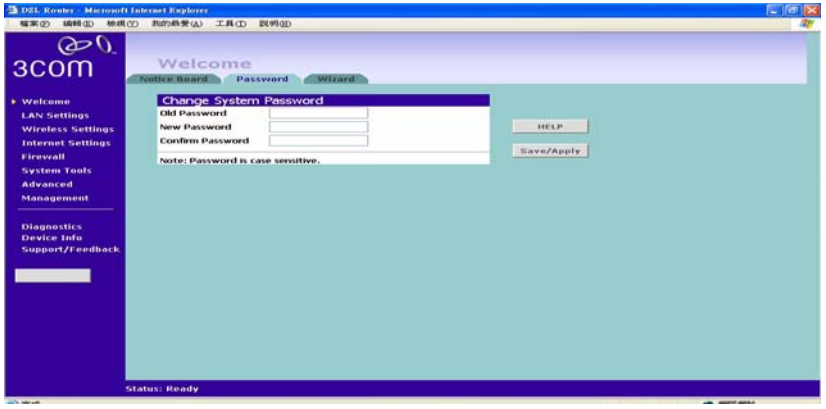
Figure 26 Notice Board Screen



The Notice Board is used to display the firmware version and configuration warning messages. For example, you would be warned if you had disabled wireless networking or wireless encryption.

Password

Figure 27 Password Screen



Changing the Administration Password

You can change the password to prevent unauthorized access to the Administration System. To do this:

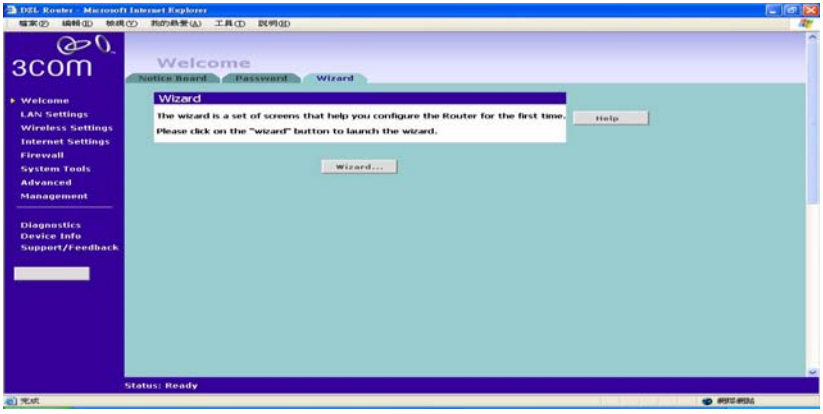
1. Enter the current password in the *Old Password* field
2. Enter the new password in the *New Password* field
3. Enter the new password again in the *Confirm Password* field
4. Click Save/*Apply* to save the new password

The password is case sensitive.

If you have forgotten your password you need to reset the Router. *See "Reset to Factory Default" on page 72.*

Wizard

Figure 28 Wizard Screen

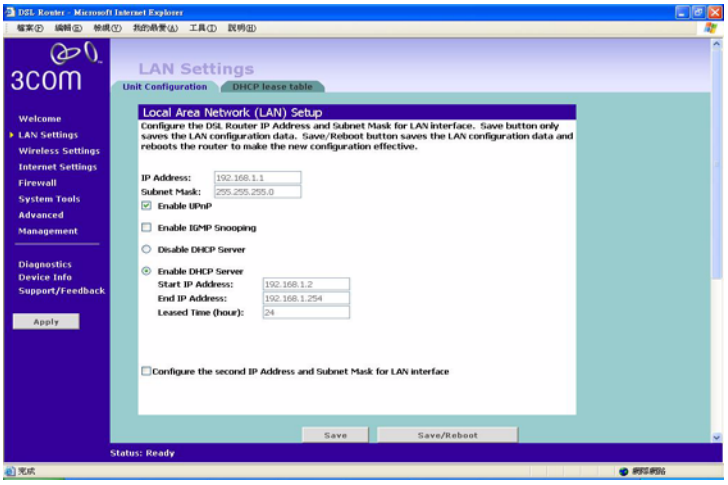


Click *WIZARD...* to launch the configuration wizard. Refer to Chapter 4 for information on how to run the wizard.

LAN Settings

Unit Configuration

Figure 29 LAN Setup Screen



This screen allows you to change the IP address and subnet mask.

1. IP Address: Enter the IP Address for your LAN interface.
2. Subnet Mask: Enter the Subnet Mask for your LAN interface.
3. Enable IGMP Snooping: The Internet Group Management Protocol snooping can snoop on IGMP query, report and leave packets transferred between IP Multicast Routers/Switches to learn the IP Multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. Select on the box to enable it.
4. Enable DHCP server on the LAN: Check this box to enable the DHCP service on the router.

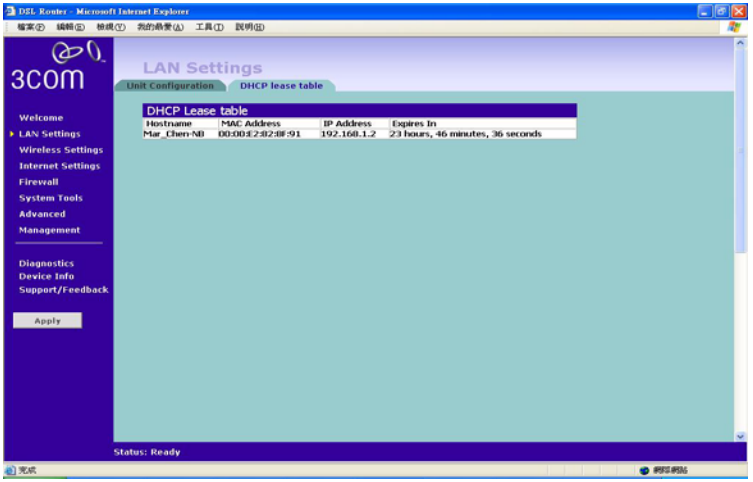
   The Firewall Router contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network.
5. Select *Enable the DHCP server* with the following settings*:* Enter the *start and end IP Address* of your DHCP range. Enter the leased time in hours to specify the frequency for DHCP assignment.
6. Configure the second IP Address and Subnet Mask for the LAN interface: Check this box to make another set of IP Address and

Subnet Mask to connect to your router if they are not included in the range of DHCP server.

7 Enter the Secondary IP Address and Subnet Mask.

DHCP Lease Table

Figure 30 DHCP Lease Table Screen



The *DHCP Lease table screen* list the client's name, MAC Address, IP Address and Expiration time which reflects the value specified in DHCP server setting in "Unit Configuration" on this chapter.

Wireless Settings

The Wireless Settings menu provides options described in the following sections.

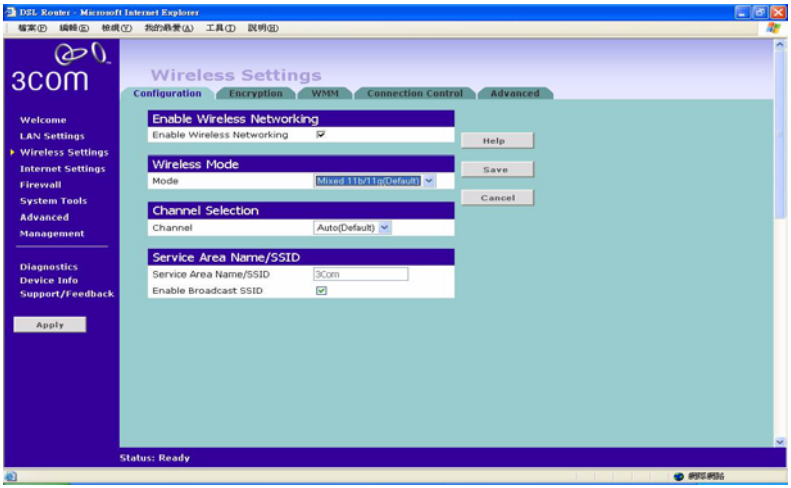
To improve the security of your wireless network, 3Com recommends that you:

1. Change the SSID from its default value - see page 52

2. Enable Encryption - see page 53

3. Enable Connection Control - see page 59

Configuration **Figure 31** Enabling Wireless Screen



Enable Wireless Networking

Use this check box to enable or disable the wireless section of your LAN. When disabled, no wireless PCs can gain access to either the Internet or other PCs on your Wired or Wireless LAN through this Router.

Wireless Mode

Select a mode from the drop-down list to configure your wireless networks. The Router supports 11b, 11g, Super G, and Mixed 11b/11g which is the default.

Channel Selection

Select a number from the drop-down list to specify which Channel the Router will transmit and receive on. If another access point or Router nearby is using the same Channel as you, there will be a reduction in the performance of your network. If this seems to be the case, you should select a different channel number. Usually the Wireless computers will scan to find the correct channel, but if they don't you must configure them to use the same Channel number as the Router.

Valid channels are country dependent. See "Channels" on page 125 for a list of channels approved by each country.

Service Area Name/SSID

This allows you to name your Wireless network. The *Service Area Name/SSID* field will accept any alphanumeric string and has a maximum length of 32 characters. Your Wireless computers must be configured with exactly the same name or you will not establish a connection. The Service Area Name may also be referred to as "ESSID" depending on your networking vendor. By default the Router uses the name "3Com". 3Com recommends that you change the default name.

In order that your wireless computers can connect to the Router, you must:

- Use Infrastructure Mode, not Ad hoc Mode.
- Have the same Service Area Name as the Router.
- Have the same Channel number as the Router.
- Use the same encryption type and keys as the Router.
- Ensure that the PC is included in the authorized Wireless PCs list if Connection Control is enabled. See page 59.

Enable Broadcast SSID

Disable this feature after you have installed your wireless network to improve the security of your network. When the check box is checked, the Router will broadcast the Service Area Name/SSID of your wireless network, which reduces the security of your Router as it allows any wireless client to see your wireless LAN.

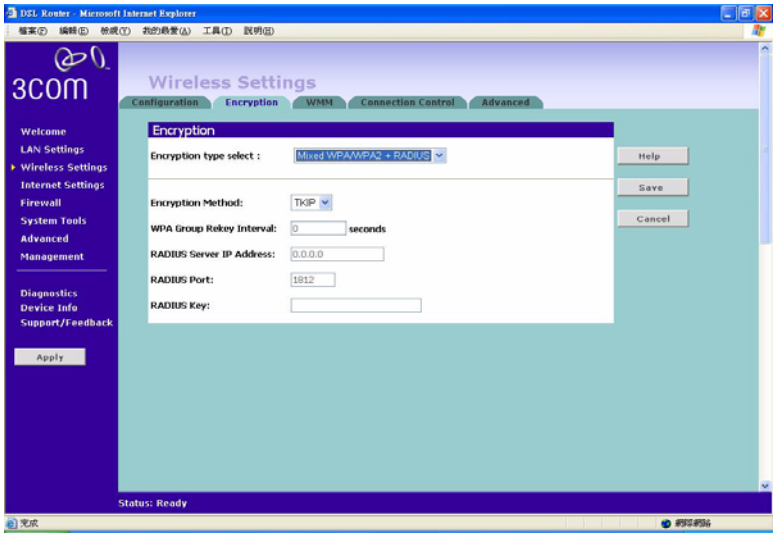
If you have a wireless client that can detect all the available SSIDs in your area, your client will not list the Router SSID unless this feature is enabled. The clients will still be able to connect, provided that they are supplied with the SSID.

3Com recommends that you install your wireless network with this feature enabled and then disable it once you have set up the Router and wireless clients.

After you have finished configuring your Router, click on Save to save your existing changes or Cancel to revert your changes.

Encryption

Figure 32 Encryption Screen



When setting up wireless networks, it is important to remember that with encryption disabled, anyone with a Wireless PC can eavesdrop on your network. 3Com recommends that you get the network working with encryption disabled first and then enable it as the last step. This will simplify setting up your network.

The Router supports two types of encryption:

- WPA/WPA2/Mixed WPA WPA2 — Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Both WPA and WPA2 use Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.11x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES). The mixed mode will let you choose the encryption mechanism interchangeably with either TKIP or AES.

- WEP — Wireless Equivalent Privacy (WEP) is a 64 bit or 128 bit encryption method with user configurable fixed keys.

WPA/WPA2/Mixed WPA WPA2 +Radius

PSK2+RADIUS features using of a RADIUS server with the pre-shared key authentication method. (This should only be used when a RADIUS server is connected to the Router).

WPA provides a higher level of security, provided by its longer key and dynamic changes made to the key over time. 3Com recommends that you use WPA with any clients which support it.

If you enable encryption on the Router, you must reconfigure your wireless PCs to use exactly the same Encryption Type and Keys otherwise the devices will not understand each other.

The encryption methods used by the Router secure data transmitted through wireless communications between the Router and its wireless clients. Enabling encryption has no security effect on data transmitted through wired (Ethernet) connections or through your connections to the Internet.

Configuring WPA/WPA2 Encryption

You can choose to use a RADIUS server to authenticate clients, or you can specify a pre-shared key.

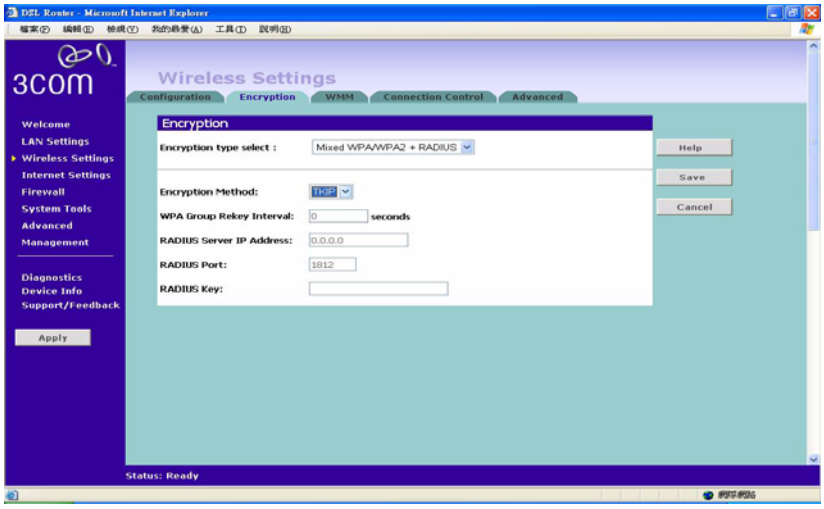
The pre-shared key is used to start the dialog between the Router and the client. During this dialog, a new key is agreed, making it more difficult to eavesdrop on wireless networks encrypted using WPA, than those encrypted using WEP.

- To use a RADIUS Server to authenticate each user before they join the network, refer to "Using the Radius Server"on page 55.

- To set up the pre-shared key, refer to "Using Pre-Shared Passphrase". on page 56.

Using the Radius Server

Figure 33 WPA/WPA2 Encryption Screen - Radius Server

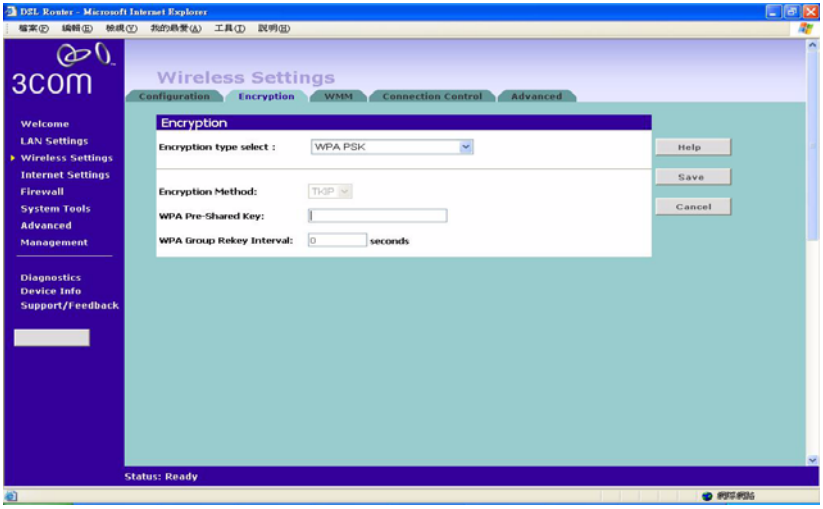


To set up WPA/WPA2/Mixed WPA and WPA2 with Radius Server:

1. Select *Encryption Method* from the drop-down box.
2. Enter the frequency for key generating in seconds.
3. Enter the *RADIUS Server IP address*.
4. Enter the *Server Port*.
5. Enter the key for the Radius Server.
6. Click *Save* to save your changes.

Using Pre-Shared Passphrase

Figure 34 WPA/WPA2 Encryption Screen - Pre-Shared Passphrase



To set up Pre-Shared Passphrase as the WPA Type:

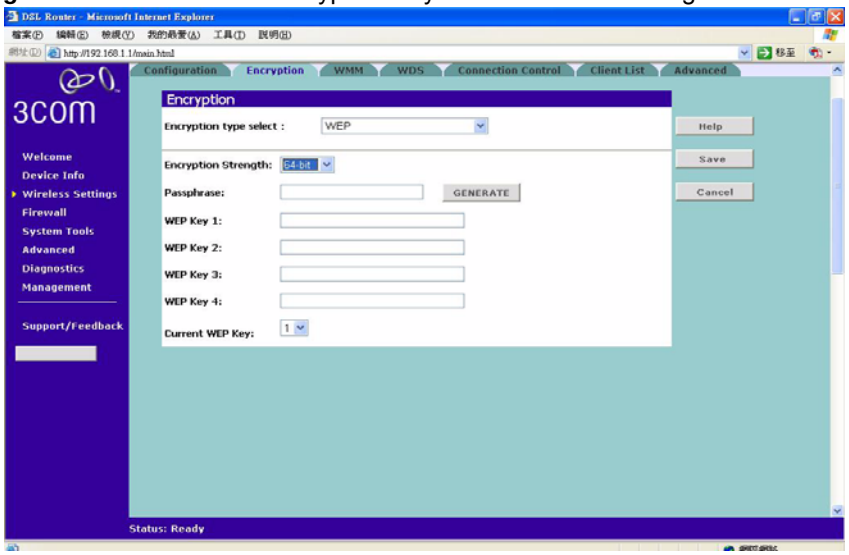
1. Select *Encryption Method* from the drop-down box. Enter a phrase of between 8 and 63 characters in length in the *Pre-Shared key* field. This passphrase will be used to generate a 256 bit key dynamically.
2. Enter the frequency for key generating in seconds
3. Click Save to save your changes.

Configuring WEP Encryption

There are two levels of WEP encryption available, 64 bit (sometimes referred to as 40 bit) and 128 bit. Use the *Encryption strength* drop-down menu to select the desired level.

Encryption Keys

Figure 35 64 bit/128 bit Encryption Keys Screen - WEP Configuration



To set up WEP encryption:

1 Select *128 bit encryption* or *64 bit encryption* from the *Encryption Strength* drop-down list.

2 Enter the passphrase which can be up to 31 characters long and may contain any alphanumeric characters in the field.

3 Click on the Generate to generate 4 hex keys automatically. Virtually all manufacturers support this scheme. Hexadecimal numbers are formed from 0-9 and A-F. In 64 bit WEP, the passphrase will generate 4 different keys. However, in 128 bit WEP, this method only generates 1 key which is replicated for all 4 keys.

If you encounter any difficulty when you enable WEP ensure that you check that each key on your wireless computer is exactly the same as each key on your Router. In other words, Key number 1 on the Wireless computer must have the same Hex number as Key number 1 on the Router, Key 2 on the Wireless computer must match Key 2 on the Router and so on.

4 Select the *Current WEP Key,* which is the key the Router uses when it transmits. You can change the selected key periodically to increase the security of your network.

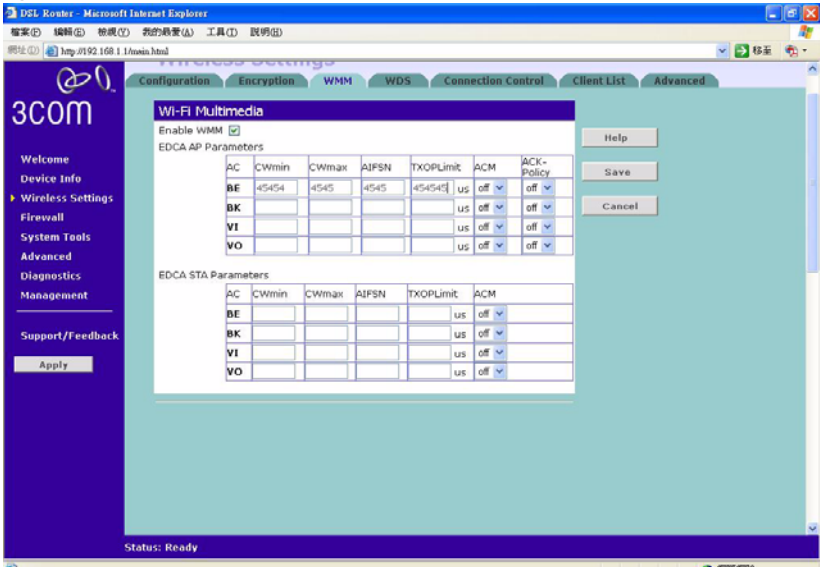
5 Click on Save to save your changes.

Some wireless adapters have only one key available on their WEP configuration page. If this is the case ensure it is the same as Key 1 on the Router and that it is selected as the Current WEP key.

WMM Wi-Fi MultiMedia QOS (Quality of Service) ensures the quality of service in wireless networks for multimedia applications. 3Com recommends that you leave the settings unchanged if you are not sure with your configuration. Changing the values may lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

WMM provides prioritized media access and is based on the Enhanced Distributed Channel (EDCA) method. The WMM screen gives two separate menus to set up the parameters; one is for Access Point and the other one is for Wireless Stations.

Figure 36 WMM Screen



Access Category - There are four types of traffics:

BK: Background

BE: Best Effort

VI: Video

VO: Voice

Enter the appropriate values for each category:

CWmin: Minimum Contention Window. It should be small for high-priority traffic.

CWMax: Maximum Contention Window. It should be small for high-priority traffic.

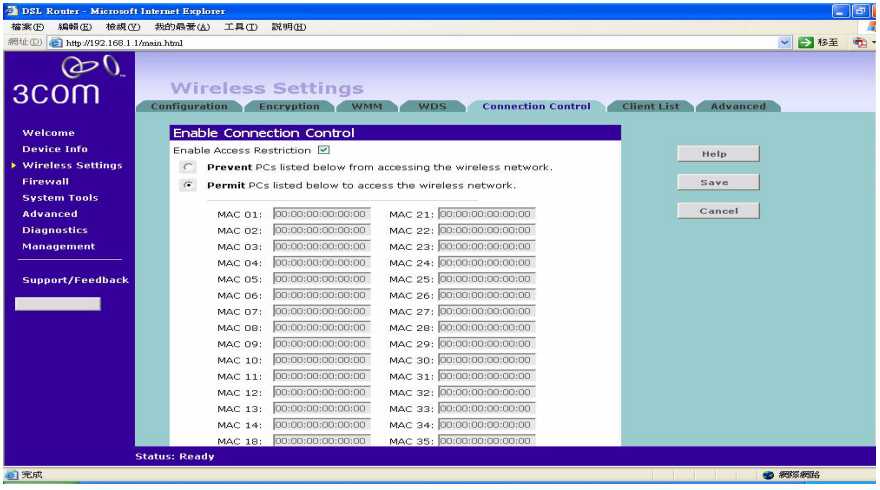
AIFSN: Arbitrary Inter-Frame Space Number, Sometimes referred to as the Random Backoff wait. This value should also be smaller for higher-priority traffic.

TXOPLimit: Transmit Opportunity Limit. Enter a number in millisecond.

ACM/ACK-Policy: Audio Compression Management support/ Acknowledgement Frame which will respond from the recipient back to the sender that data was successfully received. Can be enabled or disabled.

Connection Control

Figure 37 Connection Control Screen



A higher level of security can be achieved for your wireless network if, in addition to using encryption, you specify that only certain wireless computers can connect to the Router. By default, any wireless computer that has the same Service Area Name/SSID, channel and encryption settings as the Router can connect to it.

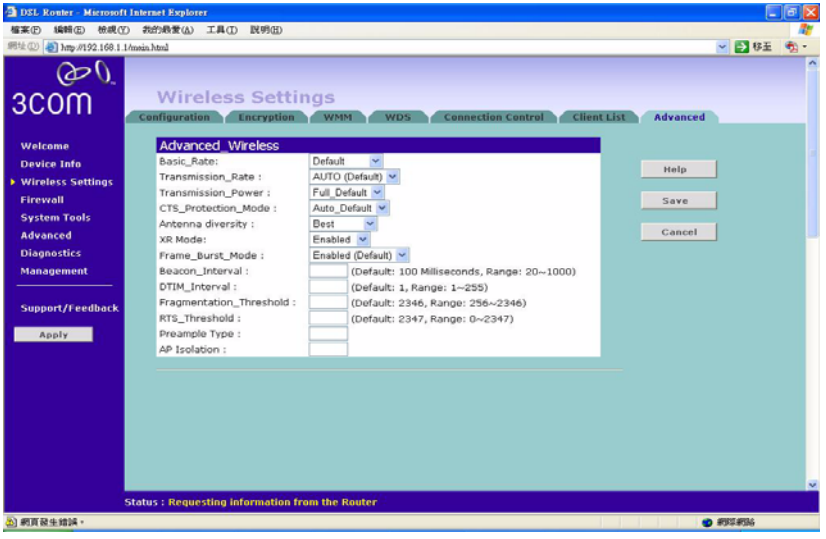
To specify that only certain wireless computers can connect to the Router, select *permit/prevent*, and then enter the MAC address of the wireless clients. If you enable this feature from a Wireless PC, it will automatically be added to the Authorized Wireless PC list. You may enter a maximum of 40 PCs in the list.

Click *Save* to save your existing configurations or *Cancel* to discard all changes.

The MAC Address must be entered as 6 hexadecimal pairs, for example 12-34-56-78-ef-ab.

Advanced Wireless Settings

Figure 38 Advanced Wireless Screen



The Advanced Wireless Settings gives you more specific and advanced options to configure your Wireless Router.

Beacon Interval: This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

XR Mode: The router embeds the Atheros Super G technology which stretches the performance of a WLAN by enabling long-range connections. Select on the drop-down list to enable this feature.

RTS Threshold (Request To Send): Should you encounter inconsistent data flow, only minor modifications are recommended.

The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU(MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.)

Fragment Threshold：defines a threshold above which the wireless packet will be split up, or fragmented. For a fragmented packet, if transmission of part of it were to be interfered with, only the portion that was successfully transmitted would need to be re-sent. Throughput will generally be lower for fragmented packets, since the fixed packet overhead consumes a higher portion of the RF bandwidth.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Internet Settings

The Internet Settings let you view your current WAN configuration and modify it. You may also add/delete new configuration.

Add a new WAN configuration: please refer to Chapter 4 on "Accessing the Wizard"

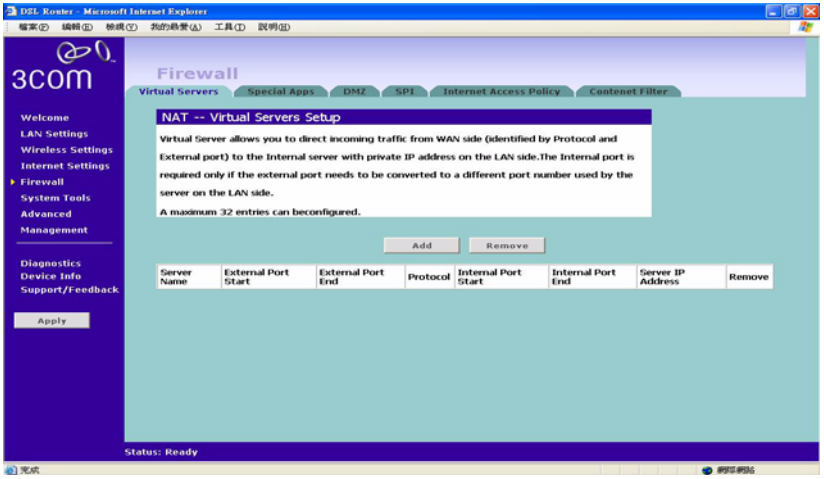
Firewall

On the main frame of the *Firewall* setup screen is a menu with six tabs: *Virtual Servers*, *Special Applications*, *DMZ*, *SPI*, *Internet Access Policy* and *Content Filter*.

Virtual Servers

Selecting the *Firewall* option on the main menu displays the Virtual Servers setup screen. (Figure 39)

Figure 39 Virtual Servers Screen



Activating and configuring a virtual server allows one or more of the computers on your network to function as a public server. For example, one of your computers could be configured as an FTP server, allowing others outside of your office network to download files of your choosing. Or, if you have created a Web site, you can configure one of your computers as a Web server, so that others can view your Web site.

To configure a virtual server:

1. Click *Add* open the *Virtual Server Settings* page.
2. Select a service from the drop-down list or type in your desired services.

3 The commonly used port with the associated service will be entered in the table automatically. You may change them manually.

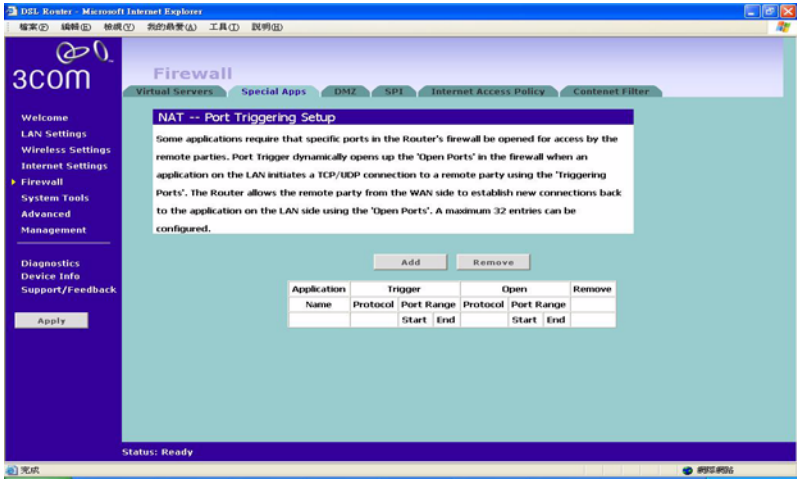
4 Click *Save/Apply* to save the settings.And the confirmed entries will be displayed.

5 Click Add to return to the Virtual Server configuration page to enter more entries.

The is a total of 32 services can be defined in the Virtual Server.

Special Applications

Figure 40 Special Applications Screen



Select *Special Apps* tab to display *NAT-Port Triggering Setup* screen. (Figure 40)

Some software applications require special or multiple connections to the Internet and these would normally be blocked by the firewall. For example Internet Telephony or Video conferences require multiple connections.

So that these special applications can work properly and are not blocked, the firewall needs to be told about them. In each instance there will be a trigger port and incoming port(s), where traffic on the trigger port tells the firewall to open the incoming ports.

Each defined Special Application only supports a single computer user, and up to 32 Special Applications can be defined. Any incoming ports

opened by a Special Application trigger will be closed after five minutes of inactivity.

To configure special applications:

1. Click *Add* open the *Virtual Server Settings* page.
2. Select a service from the drop-down list or type in your desired services.
3. The commonly used port with the associated service will be entered in the table automatically. You may change them manually.
4. Click *Save*/*Apply* to save the settings. And the confirmed entries will be displayed.
5. Click Add to return to the *Special Application configuration* page to enter more entries.

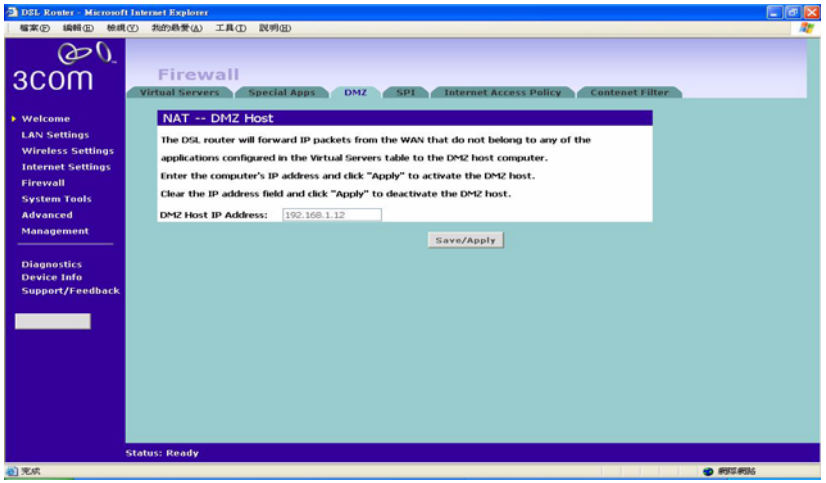
The Router will automatically allow FTP and NetMeeting sessions. You do not need to configure these as Special Applications.

Only one computer on your network can use the special application at any one time.

Virtual DMZ DMZ (De-Militarized Zone) Host is a computer without the protection of the firewall. This feature allows a single computer to be exposed to unrestricted 2-way communication from outside of your network. This feature should be used only if the Virtual Server or Special Applications options do not provide the level of access needed for certain applications.

To configure one of your computers as a DMZ host, enter the IP address of the computer in the *DMZ Host IP Address*, and then click *Save*/*Apply*.

Figure 41 Virtual DMZ Screen



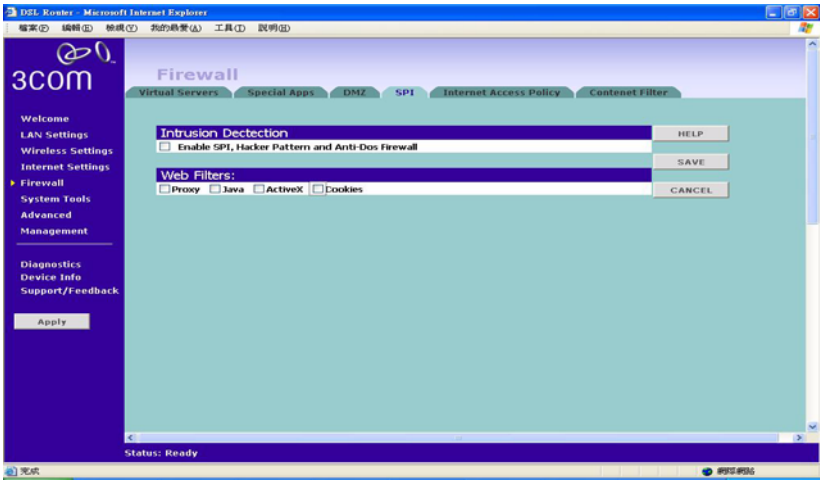
SPI Stateful Packet Inspection (SPI) inspects required blocks packets at the application layer. SPI also maintains TCP and UDP session information, including timeouts and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as DoS attacks.

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. The goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

To configure SPI information on your Router:

1 Select *Firewall* from the main menu, then select the *SPI* tab to display the SPI screen (Figure 42):

Figure 42 SPI Screen



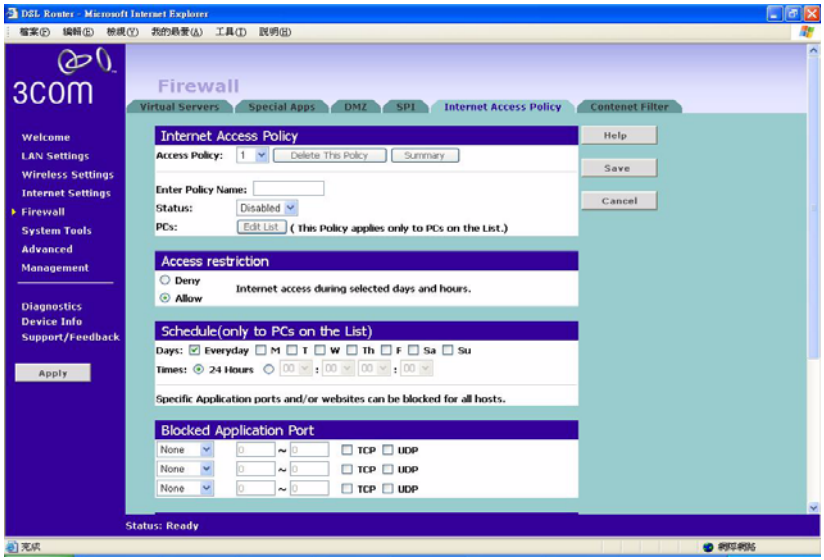
Intrusion Detection: Check on the box to enable the Stateful Packet Inspection (SPI), Hacker Pattern detection and Denial of Services (DOS) features to further guard your networks from internet attacks.

Web Filters: Check on the box to filter out the internet activities/programs from the following: Proxy, Java, ActiveX, and Cookies.

Click on Save to save your changes or Cancel to cancel your changes.

Internet Access Policy

Figure 43 The Internet Access Policy Screen



The *Internet Access Policy* screen lets you configure your Router's access availability according to specified day/time with options in blocking the application, website (URL), and website keywords.

1. Select *Access Policy number* from the drop-down menu.
2. Enter the Policy Name in the field provided.
3. Select on Status for enabling or disabling this policy.
4. The policy can be applied to a single client or a group clients.

   To do this, enter the MAC Addresses or the IP Addresses of each PC up to the total number limited by the number of the entries.Or enter the range of PC's IP Address with the last digits of their IP Addresses.

5. Select on Deny/Allow to specify your restriction types.
6. To change the schedule, check the appropriate check box for each day you want to allow access, and enter the permitted access times for each day in 24-hour clock format.

   For example, to allow access Monday through Friday between 9 am and 5 pm, check the boxes for Mon, Tue, Wed, Thu and Fri, and select

from 00:00 to 17:00 in the drop-down list for times.To allow access with different times for each day, you may have to create a new policy.

7 Select on an internet service/application to blocked the service/port number.

8 Type in the Website Accessing by URL Address with the URL that you want to block access from.

9 Type in the Website Blocking by Keyword with the keywords on the URL.

10 Click *Save* to save the settings or *Cancel* to discard them.

To assign different access rights for different computers, access status or combination with day and times:

1 Click *on the drop-down menu* for a different number of the policy. And follow the previous steps for the rest of configuration. You can create up to 10 policies.

URL Filter: To filter a specific site, enter the URL for that site. For example, to stop your users from browsing a site called `www.badsite.com`, enter `www.badsite.com` or `badsite.com` in one of these fields.

If badsite.com has multiple sub-domains, such as this.badsite.com and that.badsite.com then you can either:

■ Block them individually by entering **`this.badsite.com`** in one field and **`that.badsite.com`** in another.

or

■ Block them by entering the keyword **`badsite.com`** into one of the fields. This will block all URLs containing the string *badsite.com*. As well as blocking **`this.badsite.com`** and **`that.badsite.com`**, the keyword *badsite.com* would block searches that mentioned badsite.com in their domain name, for example **`www.notabadsite.com`**.

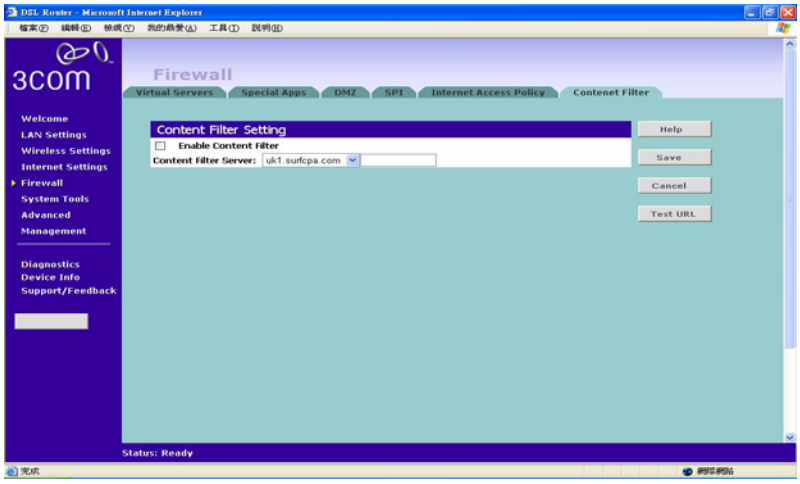
To filter a generic keyword enter it into one of the fields. You should exercise caution when choosing a keyword as many keywords are contained within other words. For example, filtering the word sex would filter the following example URLs:

- **`www.sussex.com`**
- **`www.thisexample.com`**

You can filter up to 4 keywords and URLs.

Content Filter

Figure 44 The Content Filter Screen



The content filter lets your block the websites according to pre-defined categories.

You can subscribe to the 3Com Content Filter Service, which enables you to block or allow the URLs of a number of pre-defined categories.

The Router comes with a 14-day free trial of the 3Com Content Filter Service. To activate the 14-day free trial of the service, you must first register your Router at **`www.3com.com`***. To continue using the service after the trial period, you must purchase the full 3Com Content Filter Service (3CSBCFS).*

URL filtering rules supersede content filtering rules. If the 3Com Content Filter is blocking certain Web sites that you want to allow, you can add these sites to URL Filter's allow list.

To activate Content Filtering:

1 Select *Firewall* from the main menu, then select the *Content Filter* tab.

2 Check the *Enable Content Filter* check box.

3 Select the *Content Filter Server* that you require from the drop-down list. If you select *custom entry*, enter the server IP address in the text box.

4 Select the *Server Timeout* value in milliseconds. The default is 3000 milliseconds (3 seconds).

5 Select *Allow* or *Deny* for each displayed category, as required.

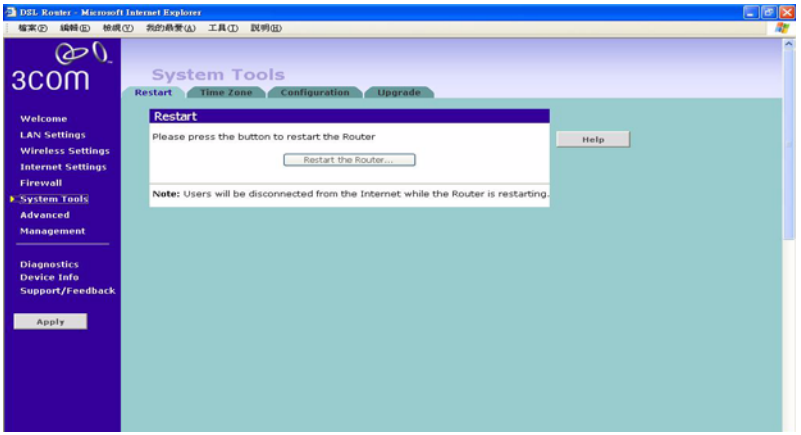
Click Save to save the settings, Test URL to test the connection with the specified content filter server or cancel to discard your changes.

System Tools

The main frame of the System Tools screen includes four administration items: *Restart, Time Zone, Configuration,* and *Upgrade* (Figure 45).

Restart

Figure 45 Restart Screen

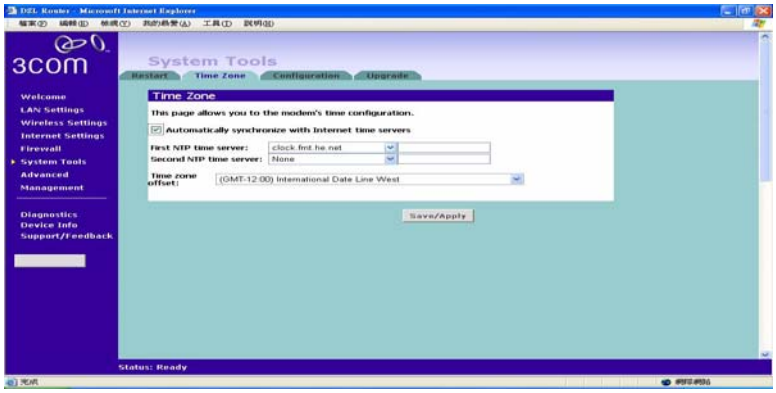


If your Router is not operating correctly, you can choose to restart the Router by selecting *Restart the Router*, simulating the effect of power cycling the unit. No configuration information will be lost but the log files will be erased. This function may be of use if you are experiencing problems and you wish to re-establish your Internet connection. Any network users who are currently accessing the Internet will have their access interrupted whilst the restart takes place, and they may need to

reboot their computers when the restart has completed and the Router is operational again.

Time Zone

Figure 46 Time Zone Screen



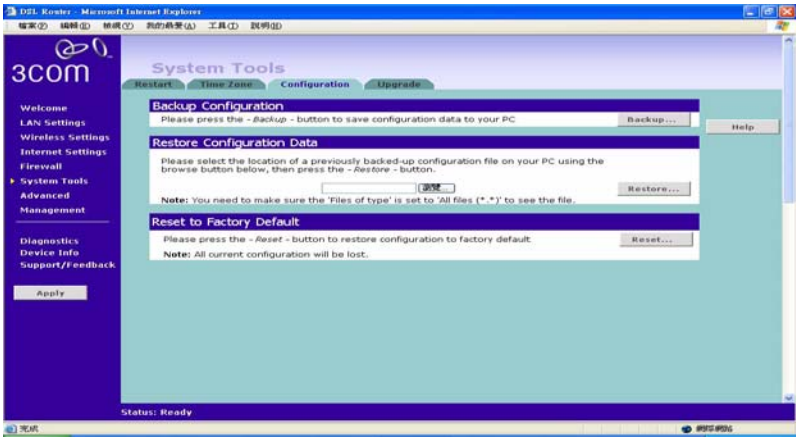
Check the *Automatically synchronize with internet time servers* to read the correct time from NTP servers on the Internet and sets its system clock automatically. You may enter two NTP servers according to your priority.

Choose the time zone that is closest to your actual location. The time zone setting is used by the system clock when displaying the correct time in the log files.

Click on *Save/Apply* to apply your settings.

Configuration

Figure 47 Configuration Screen



Select the *Configuration* tab to display the *Configuration* screen (Figure 47).

Backup Configuration

Click *BACKUP* to save the current Router configuration. You will be prompted to download and save a file to disk.

Restore Configuration Data

If you want to reinstate the configuration settings previously saved to a file, press *Browse* to locate the backup file on your computer, and then click *RESTORE* to copy the data into the Router's memory.

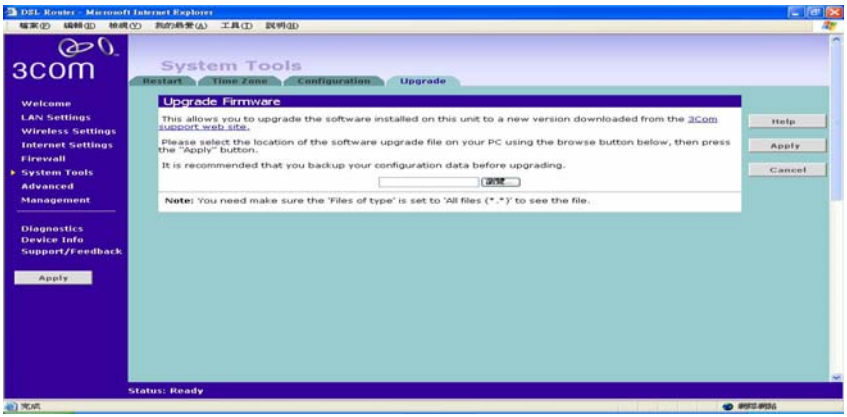
The password will remain unchanged.

Reset to Factory Default

If you want to reset the settings on your Router to those that were loaded at the factory, click RESET. You will lose all your configuration changes. The Router LAN IP address will revert to 192.168.1.1 and so are the wireless settings, and the DHCP server on the LAN will be enabled. You may need to reconfigure and restart your computer to re-establish communication with the Router.

Upgrade

Figure 48 Upgrade Screen



The Upgrade facility allows you to install on the Router any new releases of system software that 3Com may make available. To install new software, you first need to download the software from the 3Com support web site to a folder on your computer. Once you have done this, select *Browse* to tell your web browser where this file is on your computer, and then click *Apply*. The file will be copied to the Router, and once this has completed, the Router will restart. Although the upgrade process has been designed to preserve your configuration settings, it is recommended that you make a backup of the configuration beforehand, in case the upgrade process fails for any reason (for example, the connection between the computer and the Router is lost while the new software is being copied to the Router).

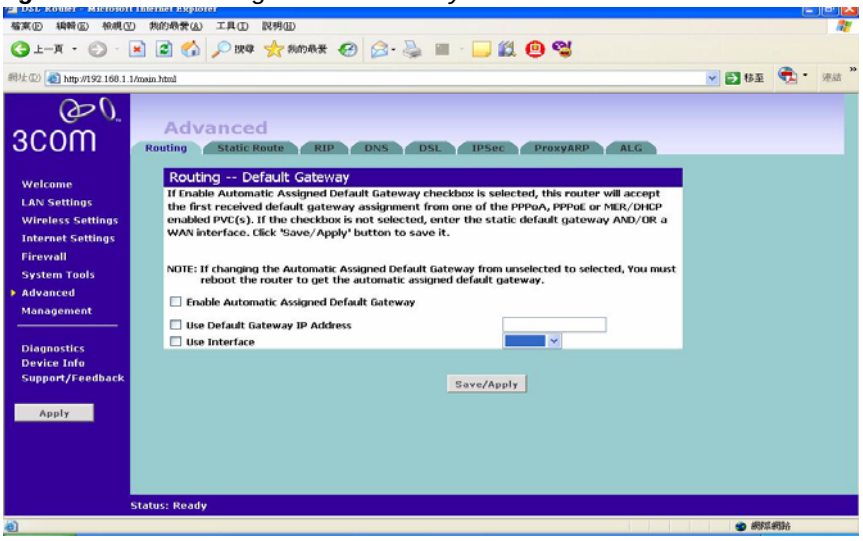
The upgrade procedure can take up to two minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Router during the upgrade procedure; if you do, the software may be corrupted and the Router may not start up properly afterwards. If the Alert LED comes on continuously after a failed upgrade, refer to Chapter 6,"Troubleshooting".

Advanced

Selecting *Advanced* from the main menu displays the following five tabs in your Web browser window: *Routing, Static Route, RIP*, *DDNS, DSL, IPSec, Proxy ARP* and *ALG*.

Routing

Figure 49 The *Routing-Default Gateway screen*

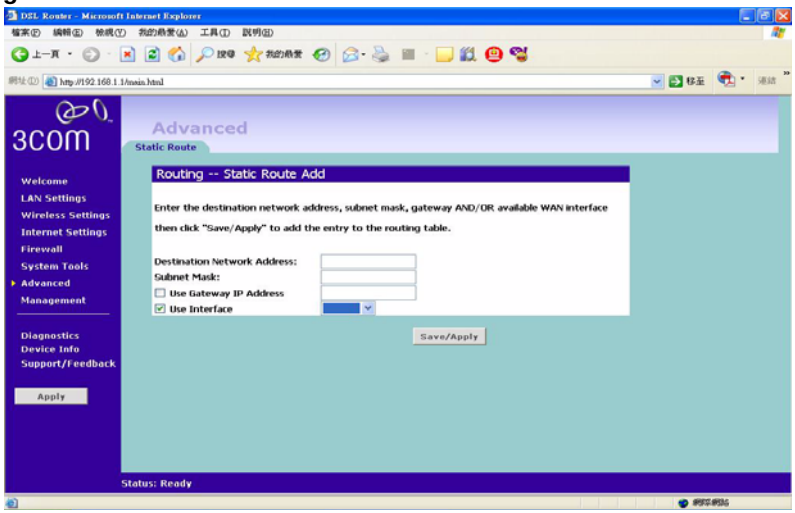


Check the box *Enable Automatic Assigned Default Gateway* to automatically assign a gateway to the router. Or you may enter the Default Gateway IP Address in the field provided and select on its associated interface.

Static Route

Router supports static route functionality. Select the *Static Route* tab to display the screen shown in Figure 50

Figure 50 Static Route screen



Please enter the following values in the box respectively to specify a static route:

- Network Address - the network address of the route. If network address and subnet mask are both set to 0.0.0.0, this is the default route.

- Subnet Mask - the subnet mask of the route. If network address and subnet mask are both set to 0.0.0.0, this is the default route.

- Gateway - the gateway used to route data to the network specified by the network address.

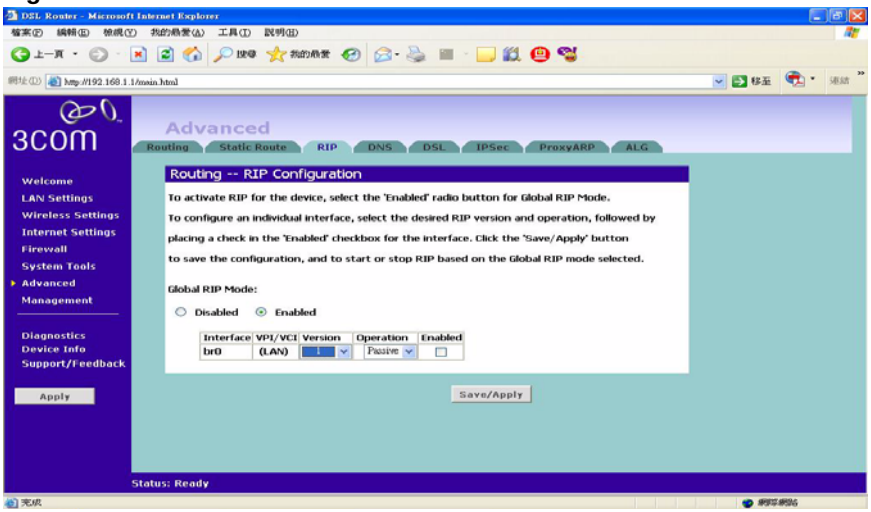
- The network interface associated with the IP address.

RIP

The Router supports the Routing Information Protocol (RIP). RIP allows you to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network. LAN and WAN interfaces can be configured independently of each other.

Select the RIP tab to display the screen shown in Figure 51

Figure 51 RIP screen

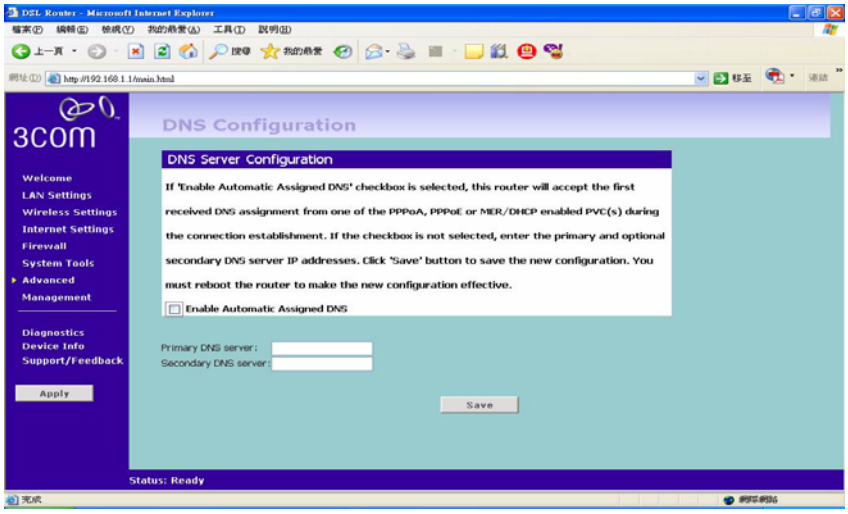


Setting Up RIP

Check the *Enable Global RIP Mode* check box check box to configure RIP on the Router.The screen displays RIP information for the LAN interface and WAN interface. To set up or change the information for one or both interfaces:

1. Select one of *Disable*, *Enable* or *Silent* from the *Operation Mode* drop-down list. If you select Enable, the Router transmits RIP update information to other RIP enabled devices. If you select Silent, the Router only receives RIP update messages.
2. Select either *1* (for RIPv1) or *2* (for RIPv2) from the *Version* drop-down list. 3Com recommends that you use RIPv1 if there is any RIP enabled device on your network that does not support RIPv2. In all other cases, select RIPv2.
3. Select either *Enable* or *Disable* from the *Poison Reverse* drop-down list. Poison Reverse is a feature that helps prevent data loops.

DNS **Figure 52** The *DNS Screen*

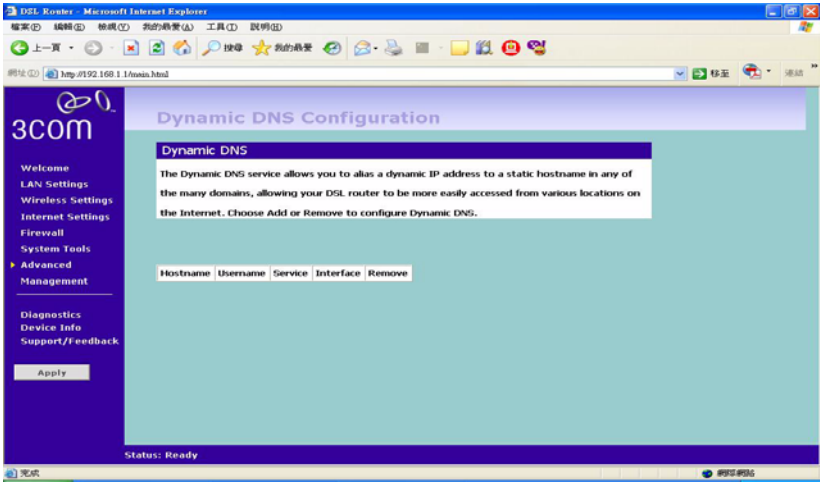

DSL Router - Microsoft Internet Explorer
http://192.168.1.1/main.html
3com
Welcome
LAN Settings
Wireless Settings
Internet Settings
Firewall
System Tools
Advanced
Management
Diagnostics
Device Info
Support/Feedback
Apply
DNS Configuration
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server:
Secondary DNS server:
Save
Status: Ready

The DNS Screen lets you specify your Domain Name Service (DNS) server's information. You may check the *Enable Automatic Assigned DNS* for automatically assigned DNS or you may manually specify your DNS server's IP Address.

DDNS Dynamic Domain Name Server (DDNS) enables you to map a static domain name to a dynamic IP address. The Router supports two DDNS providers, TZO.com and DYNDNS.org. Before you can set up DDNS, you must obtain an account, password and static domain name from your DDNS provider. DDNS is disabled by default.

To set up DDNS:

Figure 53 DDNS screen



4 Select a *DDNS Service* provider from the drop-down list. This can be either TZO.com or DynDNS.org.

TZO.com

If you select TZO.com:

1 In the *Host Name* text box, enter the host name.

2 In the *Interface* text box, select the WAN/LAN interface that will be using the DDNS.

3 In the *Username*/*E-mail* text box, enter the account name.

4 In the *Key* text box, enter the account password.

5 Click *Apply* to make this service active.

DynDNS.org

If you select DYNDNS.org:

1 In the *Host Name* text box, enter the host name.

2 In the *Username* text box, enter the account name.

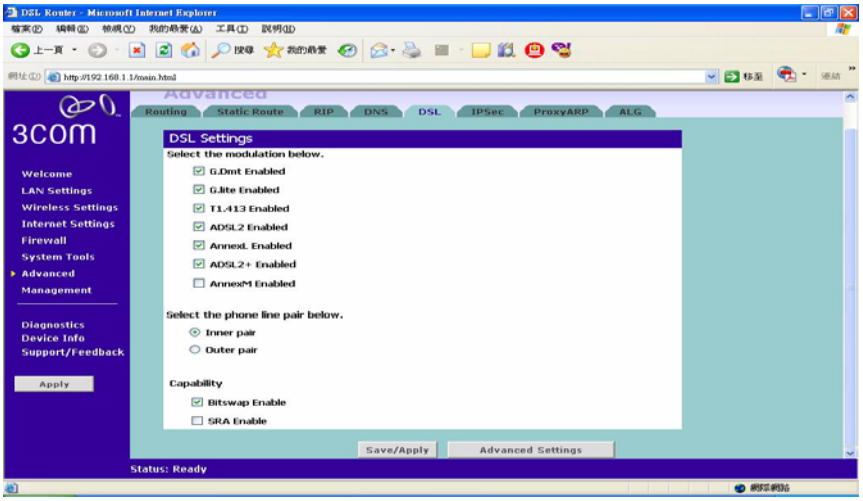
3 In the *Password* text box, enter the account password.

4 In the *Refresh Time* box, enter how often you want the service to automatically refresh, in days. The default is three days.

5 Click *Apply* to make this service active.

DSL

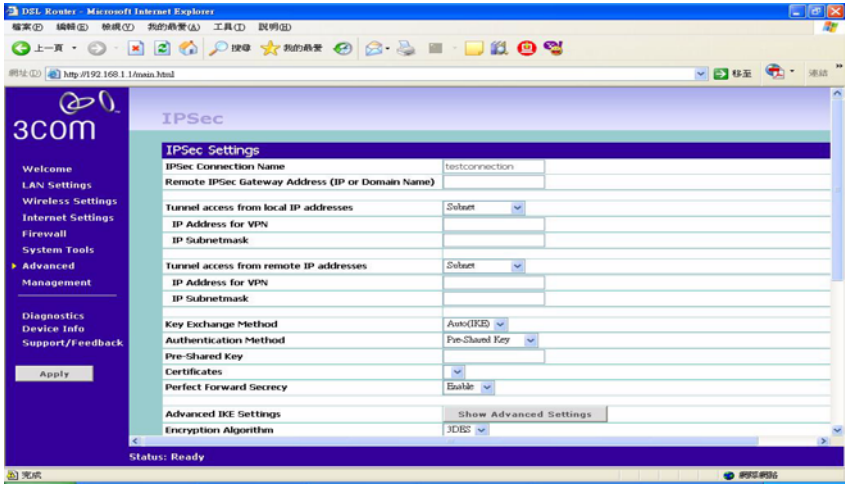
Figure 54 The DSL Setting Screen



The DSL Screen lets you configure your DSL connections. Check the boxed for the type of DSL connection that you are using. Select the type of phone line you are using. Also Check the compatibility type.

IPSec

Figure 55 IPSec Screen



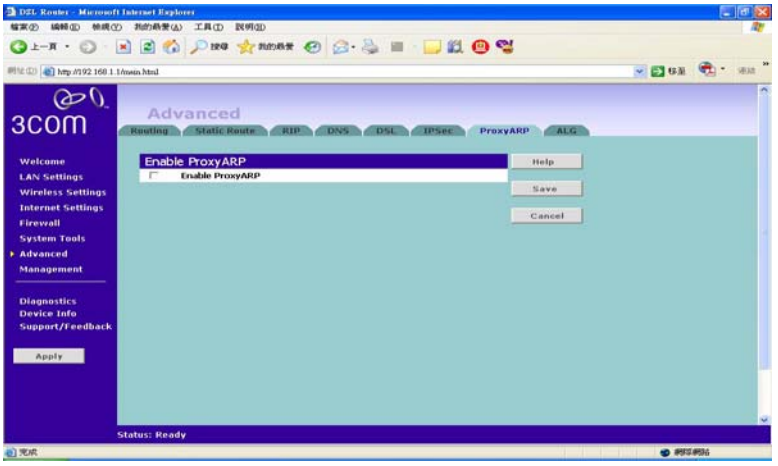
Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public

network like the Internet. The Virtual Private Network (VPN) is a popular technology used for communications between two networking sites without the expense of leased site-to-site lines.

Click on *Add New IPsec to* add new IPSec configurations. Select on the drop- down menu and enter the values in the text boxes for settings in your IPSec.

Proxy ARP

Figure 56 The Proxy ARP Screen



Proxy ARP is a variation of Address Resolution Protocol (ARP), in which an intermediate device (in this case, the Router) sends an ARP response on behalf of an end node to the requesting host. Proxy ARP can help decrease bandwidth consumption on slow-speed WAN links and allows a site to use a single IP address for two physical networks.

To use proxy ARP, you must have a range of static IP addresses assigned by your ISP.

Proxy ARP only works when the Router is assigned a static IP address.

To configure Proxy ARP:

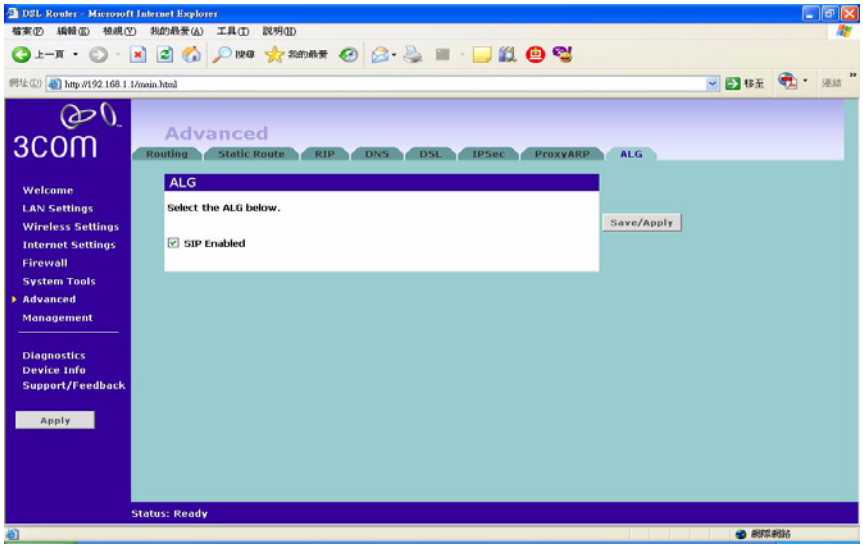
1. On the menu, click *Advanced*.
2. Click the *Proxy ARP* tab.
3. Select the *Enable Proxy ARP* check box.

4 In *IP Range From*, type the starting IP address of the IP address range that your ISP assigned to you.

5 In *To*, type the ending IP address of the IP address range.

ALG

Figure 57 The ALG Screen



An Application Layer Gateway (ALG) is a SIP Back to Back User agent (B2BUA). An ALG can be used to allow firewall traversal with SIP. If the firewall has it's SIP traffic terminated on an ALG then the responsibility for permitting SIP sessions is passed onto the ALG instead of the firewall.

It supports access control restrictions, authentication, encryption, etc.

Application layer gateways can be made for all application level protocols. They can be used for access control, but also for inter-networking, for example between IPv4 and IPv6.

Session Initiation Protocol (SIP) is a protocol developed by the IETF MMUSIC Working Group and proposed standard for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality.

Check on the box to enable the ALG feature.

Management

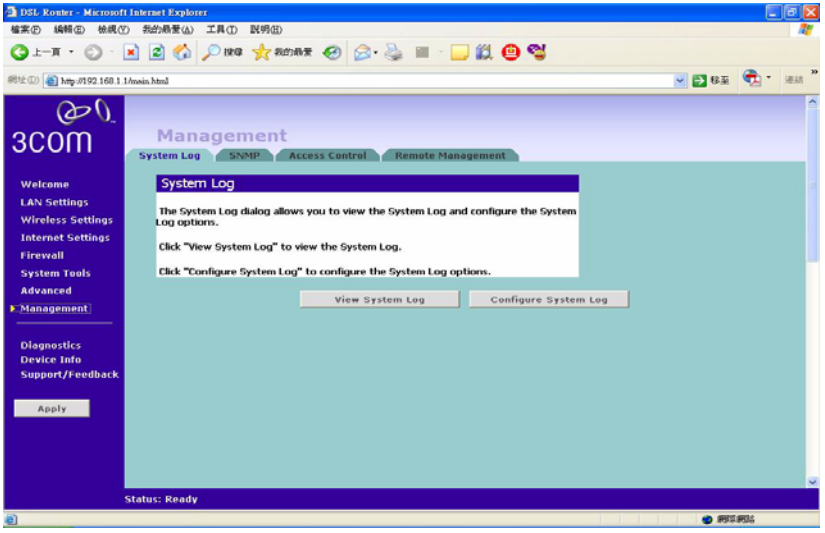
The management Screen lets you administer your routers with features such as system log, SNMP, Access Control, Remote Management.

Syslog

If you have a syslog server on the network, you can configure the Router Point to send the device logs to the server.

You may need to configure the syslog server to accept logs from the Router.

Figure 58 Syslog Screen



To view the current logs:

1 Click on the *view the syslogs* button.

To send the device logs to a syslog server:

1 Click on *Configure syslogs*.

2 Click on *Enable*.

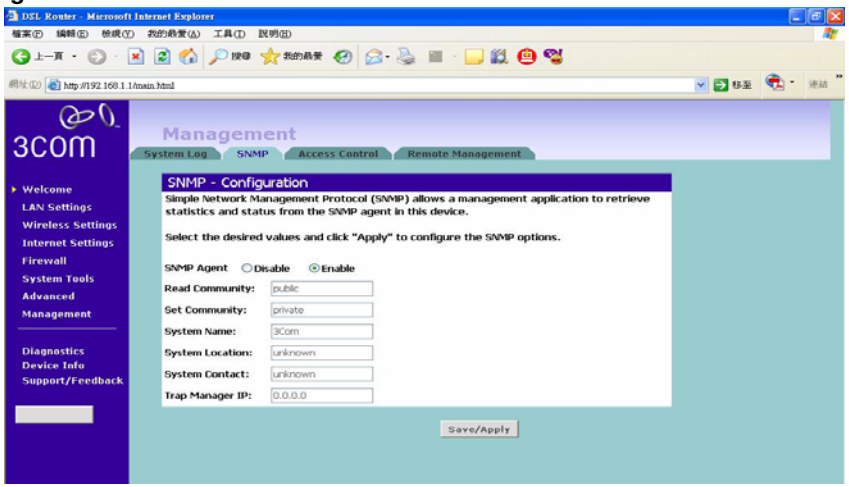
3 Select on the drop-down menu for a list of available types of logging activities.

4 Select on the Display Level for a list of available types of logging display.

5 Select on the Mode for logging mode: Local, Remote, or Both. For the remote logging, enter the remote server's IP address and Port number for receiving the logs.

SNMP

Figure 59 The SNMP Screen



Simple Network Management Protocol (SNMP) is the protocol used for exchanging management information between network devices.

Click *Enable/Disable* to enable/disable the agent.

To Configure the SNMP:

1 Type the Read Community, which is the password for the incoming Get and GetNext requests from the management station.

2 Type the Set Community, which is the password for incoming Set requests from the management station.

3 Type the System Name for the program.

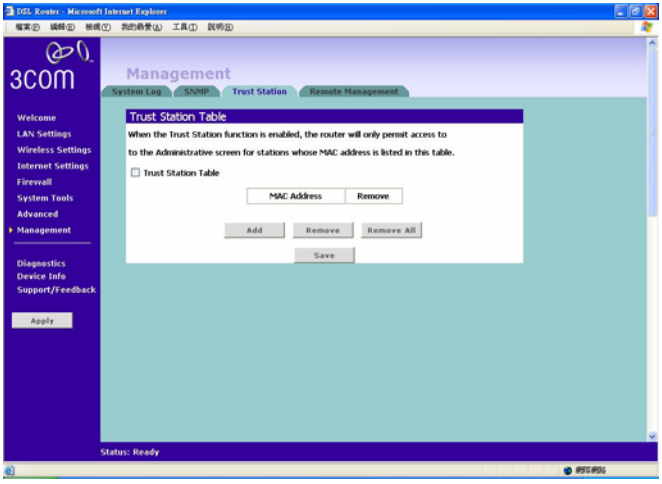
4 Type the System Location for the program.

5 Type the System Contact for the Contract person's name.

6 Type the IP Address of the station/device for sending your SNMP traps to.

Trusted Station

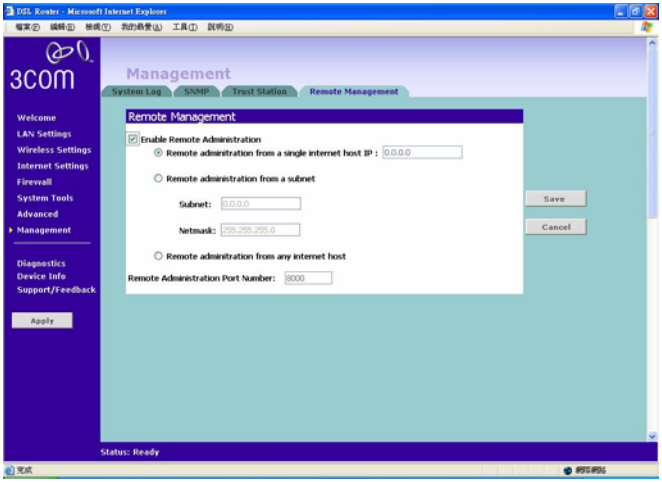
Figure 60 The Trusted Station Screen



The Trusted Station Screen let you add/remove the MAC address of the stations which can access the web administration.

Remote Management

Figure 61 The Remote Management Screen



It is possible to administer the Router remotely. Select one of the following options for remote administration:

- *Disable Remote Administration* - This option is set as default.

- *Enable administration from a **single** Internet Host* - Only the specified Host IP Address can manage the Router. Any other users will be rejected.

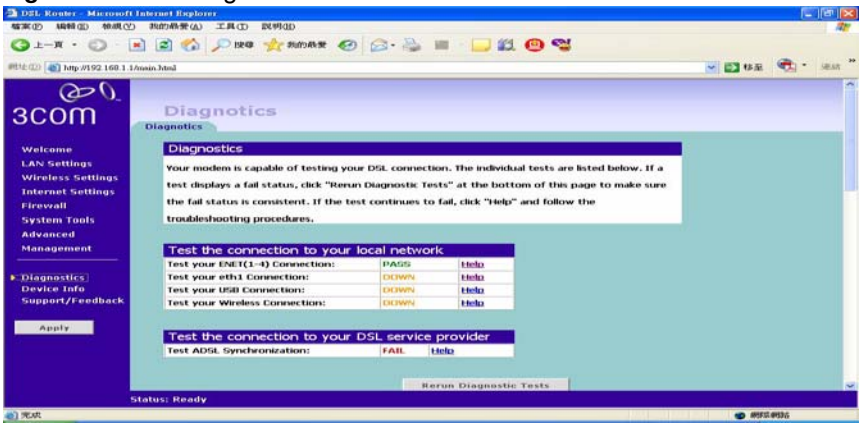
- *Enable administration from a **whole subnet*** - This option allows a number of users within the specified Host Network Address and Subnet Mask to administer the Router.

- *Enable administration from **any** Internet Host* - This option allows any host to access the administration pages.

To remotely administer your Router, enter **`http://xxx.xxx.xxx.xxx:8000`** in the location bar of the browser running on the remote computer, where *xxx.xxx.xxx.xxx* is the Internet IP address of the Router. You may then login using the administration password.

Diagnostics

Figure 62 The Diagnostics Screen


3com
Welcome
LAN Settings
Wireless Settings
Internet Settings
Firewall
System Tools
Advanced
Management
Diagnostics
Device Info
Support/Feedback
Apply
Diagnostics
Diagnostics
Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your eth1 Connection: DOWN Help
Test your USB Connection: DOWN Help
Test your Wireless Connection: DOWN Help
Test the connection to your DSL service provider
Test ADSL Synchronization: FAIL Help
Rerun Diagnostic Tests
Status: Ready

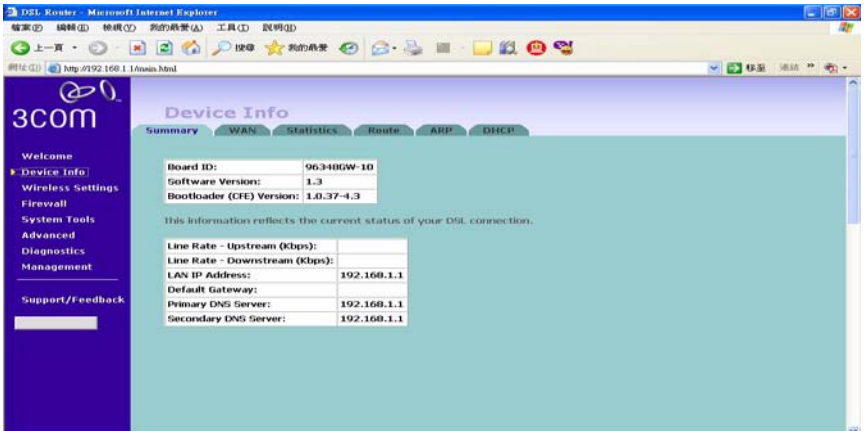
The Diagnostics Screen lets you diagnose your DSL connection and wired and wireless networkings. Click on the *Test* button to start testing.

Device Info

The Device Info Settings menu provides the following options:

Summary

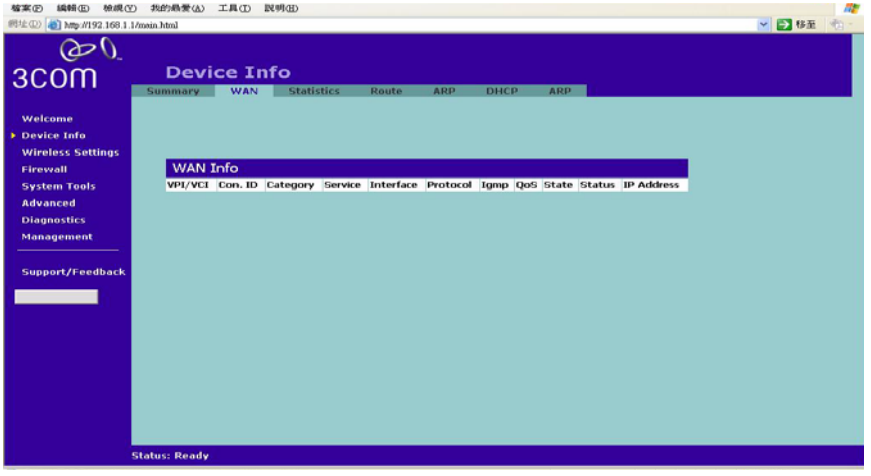
Figure 63 Summary Screen



The Summary screen is used to display the information of your LAN status.

WAN

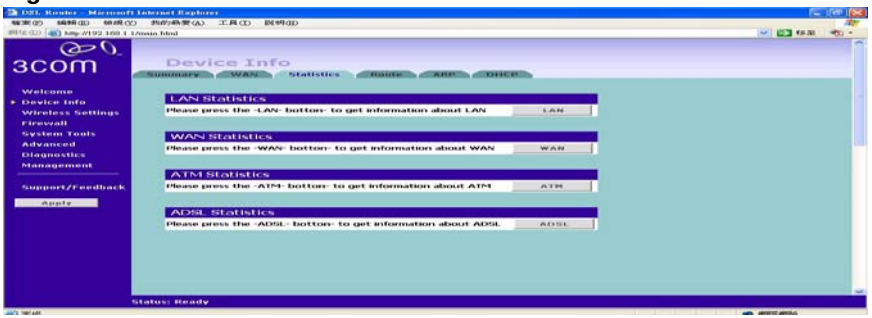
Figure 64 WAN Status Screen



The *WAN Status Screen* is used to display the information of your DSL Connection Status.

Statistics

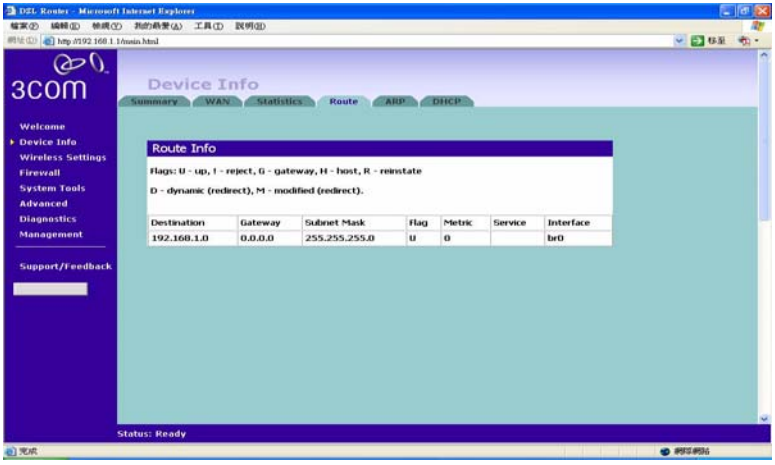
Figure 65 Statistics Screen



The *Statistics Screen* is used to display the information of your LAN/WAN/ATM/ADSL Connection Statistics. Click on the button for each connection device for more detailed information.

Route

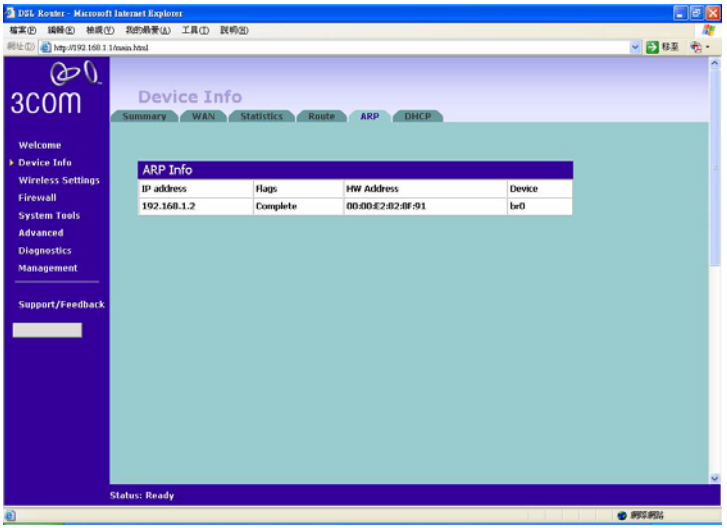
Figure 66 Route Screen



The *Route Screen* is used to display the routing status/information between your LAN and WAN. Refer to "Static Route" in this section for more information.

ARP

Figure 67 ARP Screen



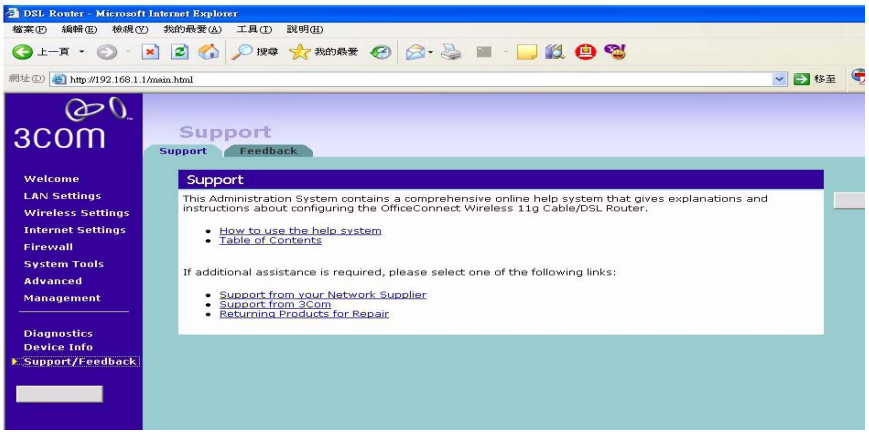
The ARP screen is used to display the Proxy ARP status. Refer to "Proxy ARP" in this section for more information.

Support/Feedback

Selecting *Support/Feedback* from the main menu displays the *Support* and *Feedback* screens.

Support

Figure 68 Support Screen



Selecting the *Support* option on the main menu displays the support links screen, which contains a list of Internet links that provide information and support concerning the Router (Figure 68).

Feedback

Figure 69 Feedback Screen

3Com - OfficeConnect Wireless Cable/DSL Router - Microsoft Internet Explorer
3COM
OfficeConnect Wireless 11g Cable/DSL Router
Feedback
Support
Feedback
Welcome
LAN Settings
Wireless Settings
Internet Settings
Firewall
System Tools
Advanced
Status and Logs
Support/Feedback
LOG OUT
Feedback
3Com is always looking for product improvements. If you'd like to help us by providing feedback you can do so by clicking on the button below which will connect you to 3Com's website.
None of the fields are mandatory - just provide the information you wish.
Please do not use this link for Technical Support. If you need assistance click on the Support option on the left hand menu.
Provide Feedback
Help
Veuillez ne pas utiliser ce lien pour contacter le Support Technique. Si vous souhaitez de l'aide, cliquez sur l'option "Support" dans le menu à gauche.
Bitte benutzen Sie dieses Link nicht für Technische Unterstützung. Sollten Sie Hilfe benötigen, klicken Sie bitte auf die 'Support' Option im linken Menü.
Vi preghiamo di non utilizzare questo link per Supporto Tecnico. Se avete bisogno di assistenza per favore fare click sull' opzione di supporto sul menu a sinistra.
Por favor, no use este enlace para recibir Soporte Tecnico. Si necesita asistencia pulse en la opcion de Soporte en el menu de la izquierda.
Status : Ready

Selecting the *Feedback* option displays the Feedback screen and allows you to provide feedback to 3Com on the operation of your

Router (Figure 69). This screen should not be used to obtain technical support.

6 TROUBLESHOOTING

Basic Connection Checks

- Check that the Router is connected to your computers and to the cable/DSL modem, and that all the equipment is powered on. Check that the LAN Status and Cable/DSL Status LEDs on the Router are illuminated, and that any corresponding LEDs on the cable/DSL modem and the NIC are also illuminated.

- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.

- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Router Configuration

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Router and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.

- Ensure that you have configured your computer as described in Chapter 3, *Setting Up Your Computers*. Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.

- When entering the address of the Router into your web browser, ensure that you use the full URL including the http:// prefix (e.g. `http://192.168.1.1`).

- Ensure that you do not have a Web proxy enabled on your computer. Go to the *Control Panel* and click on *Internet Options*. Select the *Connections* tab and click on the *LAN Settings* button at the bottom. Make sure that the *Proxy Server* option is unchecked.

- If you cannot browse to the Router, use the *winipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Router. From the *Start* menu, choose *Run* and then enter **winipcfg**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Router). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Router. Under Windows 2000, use the *ipconfig* command-line utility to perform the same functions.

- If you still cannot browse to the Router, then use the Discovery program on the accompanying CD-ROM as described in Appendix A.

Connecting to the Internet

If you can browse to the Router configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the cable/DSL modem is OK, and that the link status LEDs on both Router and modem are illuminated.

- Confirm that the connection between the modem and the cable/DSL interface is OK.

- Ensure that you have entered the correct information into the Router configuration screens as required by your Internet Service Provider. Use the “Internet Settings” screen to verify this.

- For DSL users, check that the PPPoE or PPTP user name, password and service name are correct, if these are required. Only enter a PPPoE service name if your ISP requires one.

- For cable users, check whether your ISP requires a fixed MAC (Ethernet) address. If so, use the *Clone MAC Address* feature in the Router to ensure that the correct MAC address is presented.

- For cable users, check whether your ISP requires a fixed *Host Name*. If so, enter the required *Host Name* in the *Internet Settings* screen.

- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel* > *Internet Options* > *Connections*.

Forgotten Password and Reset to Factory Defaults

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to it's factory default configuration.

CAUTION: *All your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.*

1. Remove power from the Router.
2. Disconnect all your computers and the cable/DSL modem from the Router.
3. Using a straight through Ethernet cable, connect the Ethernet Cable/DSL port on the rear of the Router to any one of the LAN ports.
4. Re-apply power to the Router. The Alert LED will flash as the Router starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly, remove power from the Router.
5. Remove the cable connecting the Cable/DSL port to the LAN port, and reconnect one of your computers to one of the Router LAN ports.
6. Re-apply power to the Router, and when the start-up sequence has completed, browse to:

   `http://192.168.1.1`

   and run the configuration wizard. You may need to restart your computer before you attempt this.
7. When the configuration wizard has completed, you may reconnect your network as it was before.

Wireless Networking

- Ensure that you have an 802.11b or 802.11g wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 95 or higher or MAC OS 8.5 or higher.

- Verify that your wireless computers are configured to work in Infrastructure mode and not Ad Hoc mode. The Router contains an Access Point that is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Router.

- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.

- Check the status of the Router Wireless LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to "Wireless Settings" and enable wireless networking.

- Ensure that the TCP/IP settings for all devices are correct.

- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive

- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router can simultaneously support WPA and WEP encryption, but can only support one configuration of each.

- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using Wireless Connection control on the Router.

- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router. For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage. Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or the Router, or trying a different channel on the Router.

■ Sources of interference: The 2.4Ghz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices like microwave ovens for example close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.

■ Most wireless computer Adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.

■ Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the Wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

Power LED or Power Adapter OK LED Not Lit

■ Check that your Router is receiving power by looking at the status of the Power LED on the front panel and the Power Adapter OK LED on the rear panel:

■ If both LEDs are lit green then the unit is receiving power.

■ If both LEDs are unlit then no power is being supplied to the unit. Check that the power adapter is plugged into a working mains outlet

and that the mains outlet is supplying power. If the mains socket is supplying power then the power adapter or power adapter connection may be faulty. See "Replacement Power Adapters" below.

- If the Power Adapter OK LED is lit but the Power LED is unlit then there may be a fault with your unit. Contact 3Com Technical Support.

- Check that you are using the correct power adapter for your Router. You should only use the power adapter supplied with your Router.

Replacement Power Adapters

If both the Power Adapter OK LED and Power LED are off, check your power adapter connection. If the mains outlet is working and is capable of supplying power to other devices, contact 3Com Technical Support and ask for a replacement power adapter. Please quote the power adapter part number shown on the OfficeConnect power adapter you are using.

Alternatively, quote the part number for your region:

Power Adapter Part Numbers:

Part Number	Region
3C16760	US and Canada
3C16761	UK
3C16762	Europe and Middle East
3C16763	Australasia (except Japan and Korea)
3C16764	South Africa
3C16766	Japan
3C16767	Korea
3C16768	Argentina

The operating temperature for the Power Adapter is 0 ^{o}C to 40 ^{o}C (32 ^{o}F to 104 ^{o}F)

The power model name is DVS-150A10FEU & DVS-150A10FUK, manufactured by DEE VAN ENTERPRISE CO., LTD.

Alert LED

The Alert LED will flash when the Router unit is first powered up while the system software checks the hardware for proper operation. Once the Router has started normal operation, the Alert LED will go out.

■ If the Alert LED does not go out following start up, but illuminates continuously, this indicates that the software has detected a possible fault with the hardware. Remove power from the Router, wait 10 seconds and then re-apply power. If the Alert LED comes on continuously again, then a fault has been detected. Locate the copy of the Router software on the accompanying CD-ROM or 3Com web site (**`http://www.3com.com`**) and upload it to the Router to see if this clears the fault (refer to “Recovering from Corrupted Software” below). If this does not fix the problem, contact your supplier for further advice.

■ During normal operation, you may notice the Alert LED lighting briefly from time to time. This indicates that the Router has detected a hacker attack from the Internet and has prevented it from harming your network. You need take no specific action on this, unless you decide that these attacks are happening frequently in which case you may wish to discuss this with your ISP. The Router logs such attacks, and this information is available through the Status and Logs screens.

Recovering from Corrupted Software

If the Alert LED remains permanently on following power-up, it is possible that the system software has become corrupted. In this condition, the Router will enter a “recovery” state; DHCP is disabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Router unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.

The latest software is available on 3Com’s Web site at:

`www.3com.com`.

1. Remove power from the Router and disconnect the Cable/DSL modem and all your computers, except for the one computer with the software image.
2. You will need to reconfigure this computer with the following static IP address information:

- IP address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default Router address: 192.168.1.1

3 Restart the computer, and re-apply power to the Router.

4 Using the Web browser on the computer, enter the following URL in the location bar:

```
http://192.168.1.1.
```

This will connect you to the Microcode Recovery utility in the Router.

5 Follow the on-screen instructions. Enter the path and filename of the software image file.

6 When the upload has completed, the Router will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.

7 Refer to the Installation Guide to reconnect your Router to the Cable/DSL modem and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Router does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

Frequently Asked Questions

How do I reset the Router to Factory Defaults?

See "Forgotten Password and Reset to Factory Defaults" on page 93.

How many computers on the LAN does the Router support?

A maximum of 253 computers on the LAN are supported.

How many wireless clients does the Cable/DSL Router support?

A maximum of 128 wireless clients are supported.

There are only 4 LAN ports on the Router. How are additional computers connected?

You can expand the number of connections available on your LAN by using hubs, switches and wireless access points

connected to the Router. 3Com wireless access points and OfficeConnect hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

http://www.3com.com/

Does the Router support virtual private networks (VPNs)?

The Router supports VPN passthrough, which allows VPN clients on the LAN to communicate with VPN hosts on the Internet. It is also possible to set up VPN hosts on your LAN that clients elsewhere on the Internet can connect to, but this is not a recommended configuration.

Where can I download software updates for the Router?

Updates to the Router software are posted on the 3Com support web site, accessible by visiting:

http://www.3com.com

What other online resources are there?

The 3Com Knowledgebase at:

http://knowledgebase.3com.com

is a database of technical information covering all 3Com products. It is updated daily with information from 3Com technical support services, and it is available 24 hours a day, 7 days a week.

A USING THE 3COM DISCOVERY TOOL

Running the Discovery Application

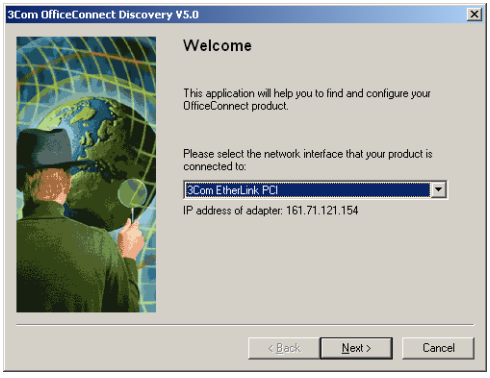
3Com provides a user friendly Discovery application for detecting the Router on the network.

Windows Installation (95/98/2000/Me/NT)

1 **Insert the Router CD-ROM in the CD-ROM drive on your computer. A menu will appear; select Router Discovery.**

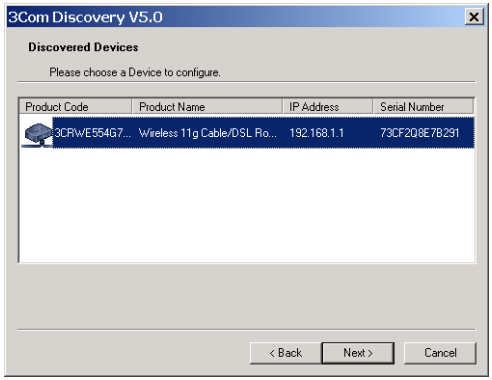
Discovery will find the Router even if it is unconfigured or misconfigured.

Figure 70 Discovery Welcome Screen


3Com OfficeConnect Discovery V5.0
Welcome
This application will help you to find and configure your OfficeConnect product.
Please select the network interface that your product is connected to:
3Com EtherLink PCI
IP address of adapter: 161.71.121.154
< Back
Next >
Cancel

2 When the *Welcome* screen is displayed click on *Next* and wait until the application discovers the Routers connected to your LAN.

Figure 71 Discovered Router Screen



3 Figure 72 shows an example Discovered Devices screen. Highlight the *Cable/DSL Router* by clicking on it, and press *Next*.

Figure 72 Discovery Finish Screen

3Com OfficeConnect Discovery V5.0
Completing the OfficeConnect Discovery Application
Communication with your OfficeConnect Device has been successful.
You are now ready to configure the Device using its set-up Wizard.
If you lose contact with the Device you should re-launch the Discovery application.
To exit the application and launch the set-up Wizard for your Device, click Finish.
< Back
Finish
Cancel

4 Click on *Finish* to launch a web browser and display the login page for the Router.

B IP ADDRESSING

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

Managing the Router over the Network

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is ‘192.168.100.8’. However, the size of the network determines the structure of this IP Address. In using the Router, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of ‘192.168.100.8’ is split into two parts:

- Part one (‘192.168.100’) identifies the network on which the device resides.
- Part two (‘.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.255.0’.

See Table 3 for an example about how a network with three computers and a Router might be configured.

Table 3 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Router	192.168.100.72	255.255.255.0

Type Two

In larger networks, where there are more devices, the IP address of ‘192.168.100.8’ is, again, split into two parts but is structured differently:

- Part one (‘192.168’) identifies the network on which the device resides.

- Part two (‘.100.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

See Table 4 for an example about how a network (only four computers represented) and a Router might be configured.

Table 4 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Router	192.168.002.72	255.255.0.0

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows® 95, Windows 98 or Windows NT 4.0. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000.

C SAFETY INFORMATION

Important Safety Information

***WARNING**: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit:

***WARNING**: The Router generates and uses radio frequency (rf) energy. In some environments, the use of rf energy is not permitted. The user should seek local advice on whether or not rf energy is permitted within the area of intended use.*

***WARNING**: Exceptional care must be taken during installation and removal of the unit.*

***WARNING**: Only stack the Router with other OfficeConnect units.*

***WARNING**: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.*

***WARNING**: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.*

***WARNING**: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.*

***WARNING**: There are no user-replaceable fuses or user-serviceable parts inside the Router. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.*

***WARNING**: Disconnect the power adapter before moving the unit.*

***WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.*

Wichtige Sicherheitshinweise

***VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*
Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Geräts installieren oder ausbauen:

***VORSICHT:** Der Router erzeugt und verwendet Funkfrequenz (RF). In manchen Umgebungen ist die Verwendung von Funkfrequenz nicht gestattet. Erkundigen Sie sich bei den zuständigen Stellen, ob die Verwendung von Funkfrequenz in dem Bereich, in dem der Bluetooth Access Point eingesetzt werden soll, erlaubt ist.*

***VORSICHT:** Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.*

***VORTSICHT:** Stapeln Sie das Geräts nur mit anderen OfficeConnect Gerätes zusammen.*

***VORSICHT:** Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.*

***VORSICHT:** Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.*

***VORSICHT:** Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.*

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Router haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.*

VORSICHT: *Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.*

VORSICHT: RJ-45-Anschlüsse. *Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.*

Consignes importantes de sécurité

AVERTISSEMENT: *Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes. Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:*

AVERTISSEMENT: *La Router fournit et utilise de l'énergie radioélectrique (radio fréquence -rf). L'utilisation de l'énergie radioélectrique est interdite dans certains environnements. L'utilisateur devra se renseigner sur l'autorisation de cette énergie dans la zone prévue.*

AVERTISSEMENT: *Faites très attention lors de l'installation et de la dépose du groupe.*

AVERTISSEMENT: *Seulement entasser le moyer avec les autres moyeux OfficeConnects.*

AVERTISSEMENT: *Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.*

AVERTISSEMENT: *La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.*

AVERTISSEMENT: *L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*

AVERTISSEMENT: *Il n'y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.*

AVERTISSEMENT: *Débranchez l'adaptateur électrique avant de retirer cet appareil.*

AVERTISSEMENT: Ports RJ-45. *Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.*

D END USER SOFTWARE LICENSE AGREEMENT

IMPORTANT: READ BEFORE INSTALLING THE SOFTWARE
3Com END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION (ì3COMî) TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE: 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the ìSoftwareî) and accompanying documentation (the ìDocumentationî), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING: You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union (ìEUî) resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT: This product, Software and/or technical data (collectively "Product") may contain encryption. This Product is subject to U.S. and EU export control laws and regulations and may be subject to export or import regulations in other countries, including controls on encryption products. You agree that you will not export, reexport or transfer the Product (or any copies thereof) or any products utilizing the Product in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, reexport, transfer or import the Product.

In addition to the above, the Product may not be used by, or exported or reexported to (i) any U.S.- or EU- sanctioned or embargoed country, or to nationals or residents of such countries; or (ii) to any person, entity, organization or other party identified on the U.S. Department of Commerce's Table of Denial Orders or the U.S. Department of Treasury's lists of "Specially Designated Nationals and Blocked Persons," as published and revised from time to time; (iii) to any party engaged in nuclear, chemical/biological weapons or missile proliferation activities, unless authorized by U.S. and local (as required) law or regulations.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade

secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature and developed solely at private expense. The Software is delivered as ìCommercial Computer Softwareî as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

GOVERNING LAW: This Agreement shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write: 3Com Corporation, Customer Support Information, 350 Campus Drive, Marlborough, MA 01752-3064

3Com Corporation

350 Campus Drive,

Marlborough, MA 01752-3064

Copyright © 2006 3Com Corporation and its licensors. All rights reserved. 3Com is a registered trademark of 3Com Corporation.

E ISP INFORMATION

Information Regarding Popular ISPs

WAN Types	Characteristics	Popular ISPs
Dynamic IP (Clone MAC)	Cable modem ISP, non-hostname based. Need to clone the MAC address in the Advanced tab of the Internet Settings page.	MediaOne, RoadRunner, Optimum Online, Time Warner, Charter, Adelphia, Metrocast.
Dynamic IP (Hostname)	Cable ISP, Requires Hostname to authenticate ie. cx213818-B. Need to enter the hostname in the Internet Settings page.	@Home Network, Cogoco, ComCast, Cox, Excite, Rogers, Shaw, Insight, Videotron
PPPoE (DSL)	Usually special software installed on PC, MacPOET/WinPOET, EnterNet 300. The Router has this software built in and you can remove it from your PC. You will need to enter the user name and password that your ISP provided to you in the PPPoE page of the Router. Leave the service name blank unless your ISP requires it.	Bell*, Century Tel, Citizens, Primus, Prodigy, Snet, Sprint FC, Verizon, First World, Brightnet, Earthlink, Ameritech, Covad, Mindspring, Sympatico DSL, USwest, Owest, SNet
PPTP	Cable or DSL, always on. Some European ISPs require a PPTP tunnel to authenticate their network.	KPN (Netherlands), Austria Telecom

Static (DSL)	DSL Modem, always on. Need to enter ALL IP information from ISP in the Static IP address section of the Internet Settings page.	CableSpeed, Cnet, Direct Link, Drizzle, DSL Extreme, Earthlink Wireless, Fast Point, Flashcom, GTE-WhirlWind, Heavenet, HSA Corp, I-55, InterAccess, LinkLine, Mission, Nauticom, NAS, Omitel, Onterra, Phatpipe, Rhythms, Speakeasy, Sterling, XO, Zyan
Static (Cable)	Cable Modem, Always on, ISP assigns specific IP information which needs to be entered on the “Fixed IP” page of the Router.	Cox Cable, Sprint, US Cable, Cable-Cable

*Bell includes Bell Advantage, Bell Canada, Bell South, PacBell and Southwestern Bell.

GLOSSARY

802.11b The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11g The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.

10BASE-T The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-TX The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

Access Point An Access Point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.

Ad Hoc mode Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the Router uses. (see also Infrastructure mode.)

Auto-negotiation Some devices in the OfficeConnect range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

Bandwidth The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.

Category 3 Cables One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

Category 5 Cables One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Channel Similar to any radio device, the OfficeConnect Cable/DSL Router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.

Client The term used to described the desktop PC that is connected to your network.

DDNS Dynamic Domain Name Server. A method that enables Internet users to tie their domain name(s) to computers or servers. DDNS enables a domain name to follow an IP address automatically when the IP address changes.

DHCP Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows

95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DNS Server Address DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL modem DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

Encryption A method for providing a level of security to wireless data transmissions. The OfficeConnect Cable/DSL Router and Wireless Cable/DSL Router offer a choice of encryption methods. See "WPA" and "WEP" for details.

ESSID Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the Router and each of it's wireless clients.

Ethernet A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

Ethernet Address See MAC address.

Fast Ethernet An Ethernet system that is designed to operate at 100 Mbps.

Firewall Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

Full Duplex A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

Router A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

Half Duplex A system that allows packets to transmitted and received, but not at the same time. Contrast with full duplex.

Hub A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

IEEE Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

Infrastructure mode Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)

IP Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

IP Address Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated

with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

ISP Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

MAC Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address Media Access Control Address. Also called the hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

NAT Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC) A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

Protocol A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

PPPoE Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the internet.

PVC Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up to torn down for each session.

RIP Routing Information Protocol. RIP allows an administrator to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

RJ-45 A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.

Server A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

SPI Stateful Packet Inspection. This feature requires the firewall to remember what outgoing requests have been sent and only allow responses to those requests back through the firewall. This way, un-requested attempts to access the network will be denied.

SSID Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.

Subnet Address An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

Subnet mask A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a

particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

Subnets A network that is a component of a larger network.

Switch A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TCP/IP Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

Traffic The movement of data packets on a network.

universal plug and play Universal plug and play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter A URL Filter is a feature of a firewall that allows it to stop its clients form browsing inappropriate Web sites.

VLAN Virtual Local Are Network. It states in 802.1q, the VLAN features frame format extensions to support Virtual Local Area Network tagging. A VLAN acts like an ordinary LAN, but connected devices don’t have to be physically connected to the same segment.

WAN Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

WDS Wireless Distribution System. A system that can be comprised of a bridging and/or a repeater mode. In wireless bridging, APs communicate only with each other to bridge together two separate networks. In wireless repeating, APs rebroadcast received signals to extend reach and range, at the expense of throughput. The Router uses wireless repeating.

WECA Wireless Ethernet Compatibility Alliance. An industry group formed to certify cross vendor interoperability and compatibility of 802.11b and 802.11g wireless networking products and to promote the standard for enterprise, small business and home environments. (see also 802.11b, 802.11g, Wi-Fi)

WEP Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.

Wi-Fi Wireless Fidelity. This is the certification granted by WECA to products that meet their interoperability criteria. (see also 802.11b, WECA)

Wireless Client The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network

Wireless LAN Service Area Another term for ESSID (Extended Service Set Identifier)

Wizard A Windows application that automates a procedure such as installation or configuration.

WLAN Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

WMM Wi-Fi Multimedia. The standard, which is a precursor to 802.11e, is meant to improve audio, video, and voice applications over Wi-Fi. The 802.11e standard includes quality of service mechanisms, which will allow network administrators to give priority to traffic such as voice that suffers from delays.

WPA Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.

REGULATORY NOTICES FOR THE ADSL WIRELESS 108MBPS 11G FIREWALL ROUTER

Channels

Use of the ADSL Wireless 11g Firewall Router is only authorized for the channels approved by each country. For proper installation, login to the management interface and select your country from the drop down list. Table 5 below lists the channels permitted by the local regulatory agencies:

Table 5 Channels

Channels	Country
1 - 13	Argentina, Australia, Austria, Bahrain, Belarus, Belgium, Brazil, Chile, China, Columbia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Finland, France*, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan(11g), Jordan, Liechtenstein, Lithuania, Luxembourg, Malaysia, Netherlands, New Zealand, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Russia, Saudi Arabia, Singapore, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, Uruguay, Venezuela.
1 - 11	Canada, Mexico, Taiwan, United States
1-14	Japan(11b)

* The channels available for use in France depend on the region in which you are located.

The 3Com ADSL Wireless 108Mbps 11g Firewall Router (WL-553) must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

This product contains encryption. It is unlawful to export out of the U.S. without obtaining a U.S. Export License.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate 3Com's warranty and all applicable regulatory certifications and approvals.

This product can only be used with the supplied antenna(s). The use of external amplifiers or non-3Com antennas may invalidate regulatory certifications and approvals.

Exposure to Radio Frequency Radiation
This device generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency exposure guidelines for an uncontrolled environment, this equipment must be installed and operated while maintaining a minimum body to antenna distance of 20 cm (approximately 8 in.).
The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's website www.hc-sc.gc.ca/rpb.
This product must maintain a minimum body to antenna distance of 20 cm. Under these conditions this product will meet the Basic Restriction limits of 1999/519/EC [Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)].

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating

instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

US – Radio Frequency Requirements

This device must not be co-located or operated in conjunction with any other antenna or transmitter.

3Com declares that WL-553 (FCC ID: O9C-WL553) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

US Federal Communications Commission (FCC) EMC Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-0034504.

3Com is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this 3Com OfficeConnect® ADSL Wireless 108Mbps 11g Firewall Router, Model Number: WL-553, or the substitution or attachment of connecting cables and equipment other than specified by 3Com.

The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

Changes or modifications not expressly approved by 3Com could void the user’s authority to operate this equipment.

REN (Ringer Equivalent Numbers) Statement

"NOTICE: The **Ringer Equivalence Number** (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5."

Attachment Limitations Statement

"Notice: This equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment with the Industry Canada certification number. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate."

US Manufacturer’s FCC Declaration of Conformity

3Com Corporation
350 Campus Drive
Marlborough, MA 01752-3064, USA
(508) 323-5000
Date: April 30, 2006
Declares that the Product:
Brand Name: 3Com Corporation
Model Number: WL-553

Equipment Type: 3Com OfficeConnect® ADSL Wireless 108Mbps 11g Firewall Router

Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

3Com OfficeConnect® ADSL Wireless 108 Mbps 11g Firewall Router

Model WL-553

Industry Canada – RF Compliance

This device complies with RSS 210 of Industry Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.

L ‘ utilisation de ce dispositif est autorisée seulement aux conditions suivantes: (1) il ne doit pas produire de brouillage et (2) l’ utilisateur du dispositif doit étre prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful

communication. To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Pour empecher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit etre utilize a l'interieur et devrait etre place loin des fenetres afin de Fournier un ecram de blindage maximal. Si le matriel (ou son antenne d'emission) est installe a l'exterieur, il doit faire l'objet d'une licence.

Industry Canada – Emissions Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conform à la norme NMB-003 du Canada.

Safety Compliance Notice

This device has been tested and certified according to the following safety standards and is intended for use only in Information Technology Equipment which has been tested to these or other equivalent standards:

UL Standard 60950-1

CAN/CSA C22.2 No. 60950-1

IEC 60950-1

EN 60950-1

EU Compliance

Usage restrictions apply.
See documentation

This equipment may be operated in

AT	BE	CY	CZ	DK	EE	FI	FR
DE	GR	HU	IE	IT	LV	LT	LU
MT	NL	PL	PT	SK	SI	ES	SE
GB	IS	LI	NO	CH	BG	RO	TR

Intended use: ADSL 108Mbps 802.11g/b Firewall Router

For connection to ADSL networks

NOTE: To ensure product operation is in compliance with local regulations, select the country in which the product is installed. Refer to 3Com OfficeConnect® ADSL Wireless 108Mbps 11g Firewall Router User Guide.

English	Hereby, *3Com Corporation*, declares that this *RLAN device* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	*3Com Corporation* vakuuttaa täten että *RLAN device* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart *3Com Corporation* dat het toestel *RLAN device* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze verklaart *3Com Corporation* dat deze *RLAN device* voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente *3Com Corporation* déclare que l'appareil *RLAN device* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE Par la présente, *3Com Corporation* déclare que ce *RLAN device* est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Swedish	Härmed intygar *3Com Corporation* att denna *RLAN device* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede *3Com Corporation* erklærer herved, at følgende udstyr *RLAN device* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF

German	Hiermit erklärt *3Com Corporation*, dass sich *dieser/diese/dieses RLAN device* in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt *3Com Corporation* die Übereinstimmung des Gerätes *RLAN device* mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *3Com Corporation* ΔΗΛΩΝΕΙ ΟΤΙ *RLAN device* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Italian	Con la presente *3Com Corporation* dichiara che questo *RLAN device* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente *3Com Corporation* declara que el *RLAN device* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	*3Com Corporation* declara que este *RLAN device* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, *3Com Corporation*, jiddikjara li dan *RLAN device* jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Estonian	Käesolevaga kinnitab *3Com Corporation* seadme *RLAN device* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungarian	Alulírott, *3Com Corporation* nyilatkozom, hogy a *RLAN device* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Slovak	*3Com Corporation* týmto vyhlasuje, že *RLAN device* spa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	*3Com Corporation* tímto prohlašuje, že tento *RLAN device* je ve shod se základními požadavky a dalšími píslušnými ustanoveními smrnice 1999/5/ES.
Slovene	Šiuo *3Com Corporation* deklaruoja, kad šis *RLAN device* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Lithuanian	Šiuo *3Com Corporation* deklaruoja, kad šis *RLAN device* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo *3Com Corporation* deklar, ka *RLAN device* atbilst Direktvas 1999/5/EK btiskajm prasbm un citiem ar to saisttajiem noteikumiem.

A copy of the signed Declaration of Conformity can be downloaded from the Product Support web page for the 3Com OfficeConnect® ADSL Wireless 108Mbps 11g Firewall Router at http://www.3com.com.

Also available at
http://support.3com.com/doc/WL-553_EU_DOC.pdf

EU – Restrictions for Use in the 2.4GHz band

The device may be operated indoors in all countries of the European Community using the 2.4GHz band: Channels 1 – 13.

Brazil RF Compliance

Este equipamento opera em caráter secundário, isto é, no tem direito a proteço contra interferncia prejudicial, mesmo de estaços do mesmo tipo, e no causar interferncia a sistema operando em caráter primário.

INDEX

Numbers
802.1q 36

A
Access Rights 68
Addresses
  IP 103
Administration Password 32, 48
Advanced 73
  DDNS 77
  RIP 75
  routing table 77
  static route 74
Automatic Addressing 105

C
Channels 125
Configuration
  backup 72
  restore 72
content filtering 69
Conventions
  notice icons, About This Guide 8
  text, About This Guide 8
Country Selection 30

D
DDNS 77, 78
DHCP 40, 49, 86, 105
DHCP Server 27
Discovery Application 101
DNS 26, 37, 38
  primary 37, 38
  secondary 37, 38
DoS attacks 65
Dynamic IP Address 37, 62

E
Enable 802.1q 36
encryption 53
  WEP 53
  WPA 53

F
Firewall 62
  SPI 65, 66
Forgotten Password 93

I
Internet
  addresses 103
IP Address 22, 39, 103

L
LAN 39, 49
LED 15
Login 102

M
MAC Address
  modifying 60

N
Network
  addresses 103
Networking
  wireless 94
NIC
  wireless 15
Nitro Mode 53

P
Password 29, 47
PC Privileges 65
PPPoE 28

R
Radius 55
Radius Server 55
Remote Administration 84
Reset to Factory Defaults 72, 93

Restart 70
RIP 75
    setting up 76

S

Safety Information 20
security
    remote administration 84
Setup Wizard 29, 48
Special Applications 63
SPI 65
Static Addressing 105
static route 74
Subnet Mask 39, 103
Summary 42
Support Information 88
Support Links 89

T

TCP/IP 25, 27, 40, 49, 103
Time Zone 33, 71

U

Unit Configuration 86
Upgrade 73
URL Filter 68

V

Virtual Servers 62
VLAN 36

W

Web Proxy 28
Wireless
    channel selection 51
    configuration 51
    connection control 59
    encryption 53
    LED 16
    networking 94
    NIC 15
    service area name 52
    settings 41, 50
WMM 58
WPA encryption
    configuring 54

3Com Corporation, Corporate Headquarters,
350 Campus Drive, Marlborough, MA
USA 01752-3064.

To learn more about 3Com products and services, visit our World Wide Web site at **www.3com.com**

All specifications are subject to change without notice.

Copyright © 2006 3Com Corporation. All rights reserved. 3Com and OfficeConnect are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies.